2020-09

A SYSTEMATIC APPROACH TO IDENTIFYING OPPORTUNITIES FOR MAKING SYSTEMS CONTEXT AWARE TO ADDRESS SAFETY HAZARDS

Rodriguez, Jared R.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A SYSTEMATIC APPROACH TO IDENTIFYING OPPORTUNITIES FOR MAKING SYSTEMS CONTEXT AWARE TO ADDRESS SAFETY HAZARDS

by

Jared R. Rodriguez

September 2020

Thesis Advisor: James B. Michael
Co-Advisor: Marko Orescanin

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A SYSTEMATIC APPROACH TO IDENTIFYING OPPORTUNITIES FOR MAKING SYSTEMS CONTEXT AWARE TO ADDRESS SAFETY HAZARDS

5. FUNDING NUMBERS

6. AUTHOR(S) Jared R. Rodriguez

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Context aware systems sense the state of their environment and adapt their behavior accordingly. Implementing context awareness in mission-critical systems can potentially mitigate hazards that arise in legacy systems. This thesis presents a systematic approach to apply safety analysis to identify opportunities for mitigating safety risk through mapping context-awareness capabilities to identified safety hazards.

14. SUBJECT TERMS
software system safety, context awareness

15. NUMBER OF PAGES
81

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A SYSTEMATIC APPROACH TO IDENTIFYING OPPORTUNITIES FOR MAKING SYSTEMS CONTEXT AWARE TO ADDRESS SAFETY HAZARDS

Jared R. Rodriguez
Lieutenant Commander, United States Navy
BS, U.S. Naval Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2020

Approved by: James B. Michael
Advisor

Marko Orescanin
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Context-aware systems sense the state of their environment and adapt their behavior accordingly. Implementing context awareness in mission-critical systems can potentially mitigate hazards that arise in legacy systems. This thesis presents a systematic approach to apply safety analysis to identify opportunities for mitigating safety risk through mapping context-awareness capabilities to identified safety hazards.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
AOR	area or responsibility
ASTM	American Society for Testing and Materials
ASU	aft-steering unit
BRM	bridge resource management
BTB	bridge-to-bridge very high frequency radio
CAST	causal analysis based on STAMP
CO	Commanding Officer
COLRERGS	Convention on the International Regulations for Preventing Collisions at Sea
COMNAVSURFPAC	Commander, Naval Surface Forces Pacific
COMPACFLT	Commander, U.S. Pacific Fleet
DARPA	Defense Advanced Research Projects Agency
DDG	Guided Missile Destroyer
DS	data science
IBNS	Integrated Bridge and Navigation System
JSM	USS *John S. McCain*
ML	machine learning
MV	motor vessel
NN	neural network
NOSSA	Naval Ordnance Safety and Security Activity
NTSB	National Transportation Safety Board
OOD	Officer of the Deck
OPNAVINST	Office of Chief of Naval Operations Instructions
SCC	steering control console
STAMP	Systems-Theoretic Accident Model and Processes
TSS	traffic separation scheme
USINDOPACOM	Commander, U.S. Indo-Pacific Command
XAI	explainable artificial intelligence
XO	Executive Officer

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Thank you, Professor Michael, for the seemingly unlimited amount of patience you had with me. Forever grateful. Also, a big thanks to Professor Orescanin for helping during this process and making sure I made it across the finish line.

To my beautiful wife, you are the most amazing person I know, and I would not have been able to maintain my sanity these past few years without you by my side. I love you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The demand signal is growing for intelligent systems within the U. S. Department of Defense (DOD) in response to the ongoing great-power competition. The People's Republic of China and the Russian Federation are investing in advanced technologies, including pushing the frontiers of the triad of artificial intelligence (AI), machine learning (ML), and data science (DS), in addition to operationalizing the triad in combat and related defense systems.

However, nothing comes for free. All three parts of the triad introduce complexity into systems. For instance, a deep-learning neural network (NN) can do well at performing classification-based learning for certain types of tasks performed by drones, but it is difficult for a human to determine the set of rules the NN uses to classify data items. In recognition of this and related challenges associated with machine-based classification and reinforcement learning, the U.S. Defense Advanced Research Projects Agency (DARPA) established the Explainable AI (XAI) program, with the aim of enabling warfighters "to understand, appropriately trust, and effectively manage an emerging generation of artificially intelligent machine partners" [1].

Within the U.S. Navy, artificially intelligent machine partners are being incorporated into systems that control and release energy, particularly combat and weapons systems. If that energy is released in an unsafe manner, injury, death, property damage, or environmental damage may result. Ensuring system safety is an important ingredient that goes into being able to trust in the dependability of an artificially intelligent machine partner. However, how will the U.S. Navy evaluate the system safety afforded for instance by a warship that has Sailors partnering with one or more artificially intelligent machines such as weapons systems and the ship's integrated bridge system? Introduction of AI and ML into the naval fleet poses safety-related risk that must be evaluated and considered in light of mission-readiness and mission-effectiveness requirements.

B. SCOPE OF THE THESIS

This thesis explores the safety aspects of operationalizing AI in naval shipboard systems. In particular this thesis identifies how modern system safety engineering can be used to analyze systems controlling energy that are expected to partner with the Sailor by perceiving at some level his or her environment, situation, and context.

To break ground in this uncharted area of research, this thesis consists of a case study of a real shipboard system that relies on human-machine partnering. The case study consists of applying a modern accident analysis model on an actual accident that occurred at sea that at the core seemed to be a result of system-complexity challenges. Based on the findings from the model and analysis, the thesis introduces a notional system that has a layer of context awareness to address the safety deficiencies identified in the real system. The thesis concludes with a discussion of challenges and avenues for using contextual AI while ensuring that the overall system provides an acceptable level of safety.

C. KEY FINDINGS

Key findings from this research is as follows:

1. A framed systematic approach to safety engineering: The approach uses Nancy Leveson's methodology to characterize where the hazards exist within the hierarchical control structure of a system. Then one determines where in the system it would be applicable to use context awareness to mitigate the risk associated with the identified hazards.

2. A case study of applying the approach to a real-world system that experienced a mishap revealed that utilizing the STAMP method can be beneficial to the DOD.

D. CONTRIBUTION

This thesis introduces a methodology for identifying which safety-critical or safety-related functions involving human-machine teaming could benefit from improvement in the context awareness of the human and/or machine portion of human-

machine teaming. The Naval Ordnance Safety and Security Activity (NOSSA) and other DOD organizations may be able to further develop and leverage the methodology introduced in this thesis to improve their safety engineering processes and practices.

THIS PAGE INTENTIONALLY LEFT BLANK

II. APPROACH

A. THE SYSTEMS-THEORETIC ACCIDENT MODEL AND PROCESSES

Safety has not always been a key consideration when developing systems. Even today when systems are more complex than they have ever been, safety can still be somewhat of an afterthought. However, the concept of safety has been taken more seriously over the years: This can possibly be attributed to the fact that there are means available to ensure a higher level of safety. In the past, the limitations in technology and lack of advanced techniques may have resulted in dangerous jobs and tasks having to be performed by humans and the probability of an accident occurring would have most likely been higher. What if even after taking safety more seriously and including it in the overall calculus of system operations the end product is still an unsafe operation which could result in an accident?

This is the modern-day predicament we currently find ourselves in. The last 40 years have seen the most serious accidents of the century. In fact, when considering death toll and injuries, the worst accident so far in modern history occurred in 1984 with the release of a toxic chemical at a Union Carbide plant in Bhopal, India [2]. That is just one example of an accident facilitated by unsafe technology. The Therac-25, Chernobyl, Three Mile Island, and Challenger accidents were all serious, leaving indelible marks in the history books. This forces us to ask the hard question, does advancing technology introduce less safe systems? In 1995, Nancy Leveson asked the same question in her book *Safeware: System Safety and Computers*. That question was relevant in 1995 and is still relevant in 2020, as presented in the Chapter III case study.

When thinking about safety, it is a measure of risk which is defined as the possibility of loss or injury. In the context of this paper, the term loss can be thought of as an accident, which is "an unplanned and undesired loss event. That loss may involve human death and injury, but it may also involve other losses, including mission, equipment, financial, and information losses" [3]. Humans have understood the concept of risk from the beginning of time. However, the societal and environmental changes have reshaped the

way we think about and address risk [2]. During pre-industrialization people were concerned about natural risks, specifically inclement weather and all the second- and third-order effects associated with it [2]. Post-industrialization has changed the risk from not only natural risks, but to man-made risks. Over time the risk associated from naturally occurring events has significantly decreased in developed countries, but the same development that decreased that risk is now itself a source of risk. In fact, this new risk has a much larger impact on the population. “In the United States, technological hazards account for 15 - 25 percent of human mortality and have significantly surpassed natural hazards in impact, cost, and general importance” [2].

In the Department of Defense, risk is typically thought of in an operational context. Given some mission or task, what is the operational risk? Each of the services will have a unique way of measuring that risk, but in general operational risk management is standard across the services. As an example, the U.S. Navy follows a systematic, continuous, and repeatable five-step process in accordance with Office of the Chief of Naval Operations Instructions (OPNAVINST) 3500.39C Operational Risk Management [4]. Once the operational risk management cycle has been applied, a final risk assessment code will be assigned to the overall mission and the commander will be able to make a well-informed decision on whether to proceed with the mission or operation. This was just one Service’s way of evaluating operational risk, but it demonstrates that the Department of Defense is no stranger to risk evaluation. Systems our Sailors, Marines, Soldiers, and Airmen rely on everyday also need to be evaluated for risk and overall safety.

The National Aeronautics and Space Administration’s (NASA) Office of Safety and Mission Assurance define system safety as “the application of engineering and management principles, criteria and techniques to optimize safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle” [5]. One of the most challenging tasks is to find the happy medium between operational effectiveness and safety. In many engineering disciplines as well as other fields, safety and operational effectiveness are thought to be synonymous [3]. This assumption is wrong and the distinction between the two must be recognized [3]. An unsafe system can be reliable, and a safe system can be unreliable [3]. This is just one of seven assumptions Nancy

Leveson challenges. Assumptions such as the one posited by NASA possibly stem from a time when system complexity was less of a factor in the design and operation of systems. Modern-day systems are increasingly complex and how we view their properties is a critical factor in analyzing system safety.

Legacy accident analysis models utilized to understand why and how accidents occur have largely been based on failure events [3]. The complex systems humans interact with everyday require a different approach. Thinking of safety as a control problem instead of a reliability problem can make for a more robust and effective way to evaluate and create safer systems [3]. It is no longer appropriate to think of an accident as simply a series of failure events [3]. Failure events are now just additional pieces of the puzzle. Component interactions and systemic causal mechanisms must also now be included in the analysis [3]. "Losses result from component failures, disturbances external to the system, interactions among system components, and behavior of individual system components that lead to hazardous system states" [3]. We hope to achieve a better understanding of why accidents happen in the first place, and with that understanding, we can get closer to designing and implementing the necessary controls that will make today's complex systems safer [3].

Nancy Leveson introduces us to a new causality model: Systems-Theoretic Accident Model and Processes (STAMP). STAMP emphasizes enforcing behavioral constraints vice failure prevention [3]. There are three tenets to the STAMP model: (1) safety constraints, (2) hierarchical safety control structures, and (3) process models [3].

1. Safety Constraints. If or when an accident occurs it is a failure of the safety constraints that the system has in place [3]. During the design process, developers and engineers need to be cognizant of the second- and third-order effects that safety constraints create. A system failure may occur farther down the process due to the implementation of some safety constraint. There should be a tiered approach— the overall goal per se. For example, the system safety requirement is lube oil must maintain a specific temperature for optimum main propulsion diesel engine performance [3]. The next question safety engineers should be asking is,

"Ok, how do we maintain lube oil temperature?" The answer to this question will be in the next tier of safety constraints. Every sub action taken needs to be understood and the second- and third-order effects from those actions need to be accounted for. The more complex systems become the more component interactions that need to be taken into account in safety analyses. The increase in component interactions will undoubtedly increase the likelihood that hazards will arise, and the presence of those hazards can significantly increase the likelihood of an accident—possibly severe—occurring.

2. Hierarchical Safety Control Structures. The logic stems from systems theory, the idea that individual levels place constraints on the function of the level below it [3]. Clear communication between the layers is critical. The downward flow is referred to as the reference channel. It provides instructions to ensure safety constraints are in place [3]. The upward direction is referred to the measuring channel, and this enables a safety constraint feedback mechanism in the system [3]. Figure 1 demonstrates the upward/downward flow of communication.

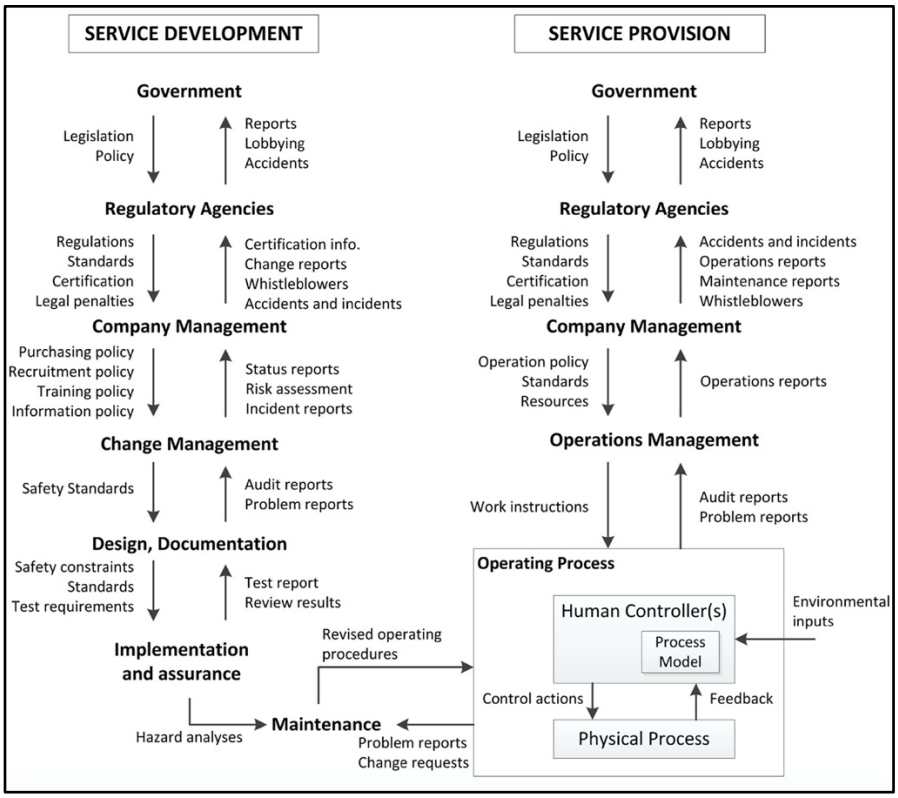


Figure 1. General model of sociotechnical control. Source: [3].

3. Process Models. Process models are part of control theory. There are four elements needed to control a process: a goal, an action condition, an observability condition, and a model condition.

> The first is a goal, which in STAMP is the safety constraints that must be enforced by each controller in the hierarchical safety control structure. The action condition is implemented in the (downward) control channels and the observability condition is embodied in the (upward) feedback or measuring channels. The final condition is the model condition: Any controller—human or automated—needs a model of the process being controlled to control it effectively. [3]

Where the model exists does not matter, but the information a model contains must all be the same [3]. Figure 2 shows the elements of the model: control laws, current state, and state transitions and provides an excellent visual. When a process does not adhere to the process model used by the controller (human or automated) an accident can occur [3].

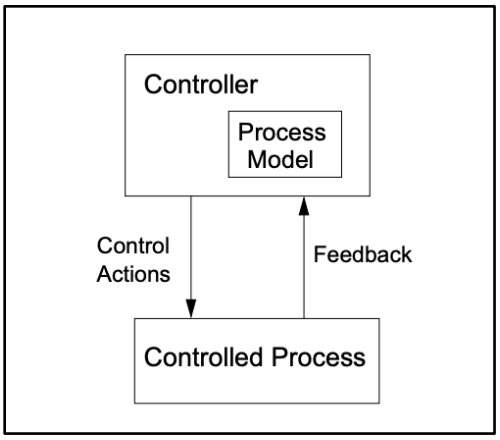


Figure 2. Controller utilizing a process model. Source: [3].

Utilizing STAMP, accidents can be better understood. STAMP provides for considering additional causes beyond vague causal explanations [3]. This is accomplished by working through the three steps just discussed: safety constraint identification, hierarchical control structure evaluation, and process model evaluation.

B. CAUSAL ANALYSIS BASED ON STAMP

STAMP is the accident causality model. The causal analysis based on STAMP (CAST) is the technique utilized to conduct the analysis of an accident that has already occurred. "In STAMP, an accident is regarded as involving a complex process, not just individual events. Accident analysis in CAST then entails understanding the dynamic process that led to the loss" [3]. CAST is a series of steps but one thing to be clear on is the order the steps are listed does not lock us into that order of execution [3]. The steps listed by [3] are as follows:

1. Identify the system(s) and hazard(s) involved in the loss.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints.
4. Determine the proximate events leading to the loss.
5. Analyze the loss at the physical system level.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level.

7. Examine overall coordination and communication contributors to the loss.
8. Determine the dynamics and the changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9. Generate recommendations. [3]

In the following chapter, CAST will be applied to an accident that took place in 2017 involving a collision at sea between a commercial tanker and a U.S. Navy Destroyer. That accident resulted in death, injury, and financial loss. The U.S. Navy should be a leader in operating safely in the maritime domain. The increased complexity in the maritime domain and the increased complexity in the sociotechnical environment that our sailors find themselves in everyday poses challenges to realizing that leadership role.

C. A NEW METHODOLOGY BASED ON STAMP

In this thesis, STAMP serves as the core of a new methodology introduced to identify safety hazards and hazard causal factors for which the risk associated with them can be mitigated via improving or introducing the context awareness of human-machine teaming. Figure 3 provides a visual depiction of the ideal workflow to implement context-awareness via STAMP. Of note, at each stage of the process there is a feedback loop to ensure a mechanism exists that allows previous work to be adjusted based on findings farther down in the process. The methodology can be the framework for future work done in this sector. This workflow can aide in increasing the safety of systems that implement complex technology. This can ultimately ensure systems that utilize human-machine teaming are safe and resilient during operations.

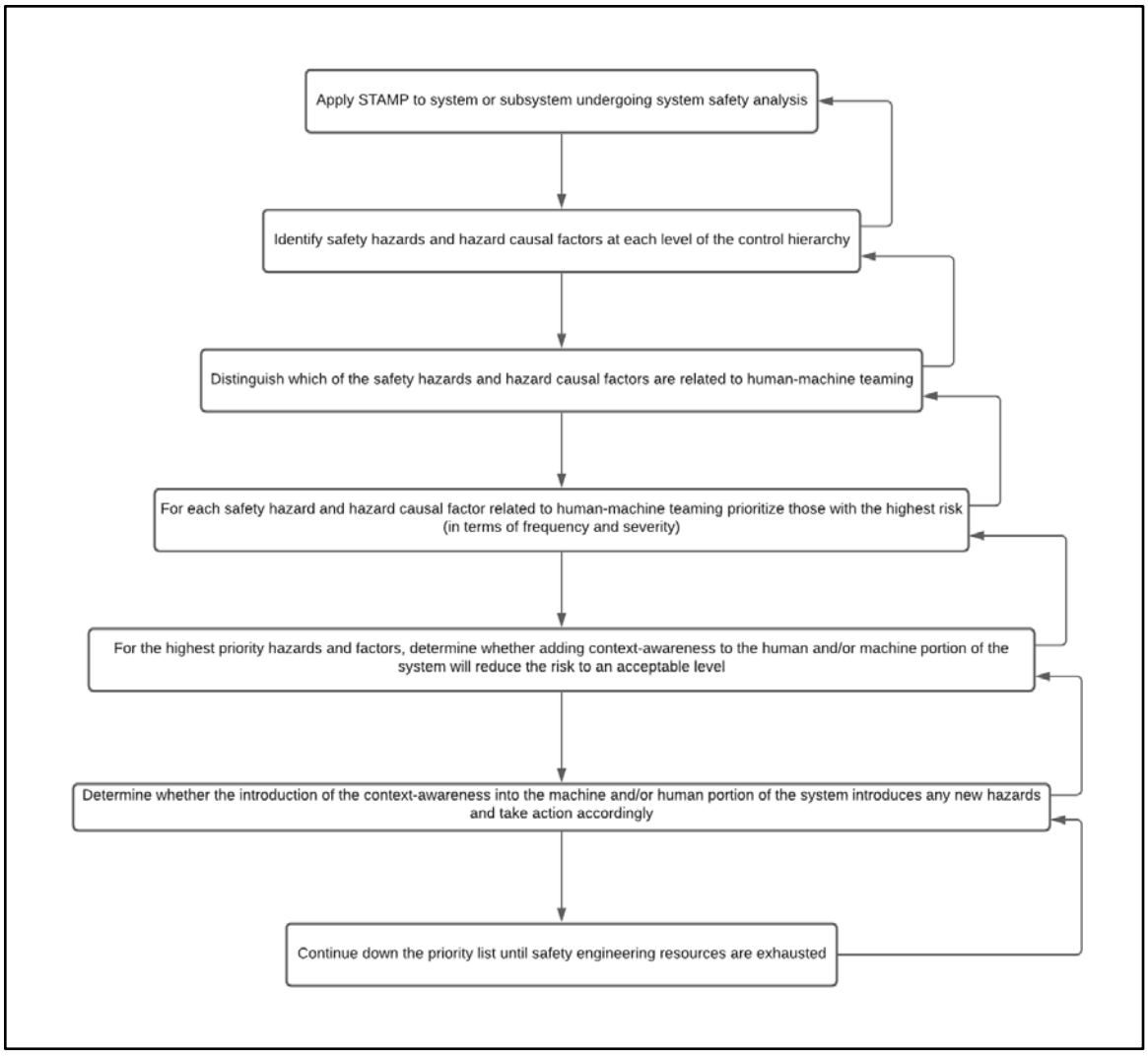


Figure 3. Methodology for extending STAMP for identifying safety hazards and hazard causal factors in human-machine teaming.

III. CASE STUDY

A. BACKGROUND

USS *John S. McCain* (DDG-56) (JSM), a Flight I DDG stationed in Yokosuka, Japan was on a six-month deployment in the SEVENTHFLT AOR during the summer of 2017. During that deployment JSM successfully completed operations in the East and South China seas as well as several port visits to countries in the region. JSM was enroute to Changi Naval Base, Singapore on 21 August 2017. The transit through the Singapore Strait commenced in the evening with overcast skies, a calm sea, and a fully operational navigation and engineering line up.

The Commanding Officer (CO) was present on the bridge since 0115, the Executive Officer (XO) since 0430, and the Sea and Anchor detail was to be set at 0600. The JSM entered the Singapore Strait around 0520 and almost immediately was posed with challenges due to the steering system. Through a series of events that will be discussed in much greater detail later on, the JSM seemingly had no control of its steering and at 0524 the JSM collided with MV ALNIC MC, a Liberian-flagged chemical tanker. Ten U.S. Navy Sailors lost their lives, 48 were injured, and the JSM sustained over $100 million in damage [6]. The full U.S. Navy report on the collision between JSM and MV ALNIC MC is in the appendix.

The hazard being controlled is at-sea collision. This hazard is on the back of every sailor's and CO's mind. An incident at sea is the fastest way to tarnish a professional reputation and, in most cases, results in being relieved of command. There exists a well-documented control structure to prevent collisions at sea. There also were traditional safety constraints in the system. However, the new technology introduced on the bridge introduced challenges and created gaps that allowed unsafe system behavior to exist. Both a U.S. Navy and National Transportation Safety Board conducted accident investigations and published their findings.

In this case study we demonstrate the feasibility of using STAMP for modeling and analyzing the accident, in addition to the added insight that STAMP provides to the user

for understanding the systemic causes in the breakdown of the safety controls in the system control hierarchy. The source of information about the accident was the official U.S. Navy investigation report [7], the National Transportation Safety Board investigation report [6], and the Comprehensive Review of Recent Surface Force Incidents [8].

Safety professionals and researchers that have first-hand experience with STAMP have found that just using the existing accident reports can produce very different views of the causality of an accident [3]. There are many more documents that could assist in the accident analysis. Technical documentation on the steering system and local operating procedures associated with each steering console would provide a deeper understanding of the incident but were not available for this case study. Traditional accident analysis tends to focus on blame, but STAMP is more about why the events occurred in the first place. By no means discrediting the importance of determining liability in accidents, but why did this occur and how can we improve processes is the real answers STAMP seeks. Liability can also be narrowed down on using a systems-theoretic approach so it can be helpful in many ways when conducting accident analysis.

B. DETERMINE THE PROXIMATE EVENTS LEADING TO THE LOSS

Breaking down the chain of events in an accident is important to understand the process model, but not necessarily the end all be all when looking to determine causality [3]. In this case study, the following chain of events will only take us to the point of the collision. There is a major damage control effort that takes place after the collision.

The events leading to the collision between JSM and MV ALNIC MC are (all times are local) [6], [7]:

<u>20 August 2017</u>

1. The JSM conducted the navigation brief for the following day's transit to Sembawang, Singapore. Based on the time, speed, and distance calculations the JSM would enter the Singapore Strait Traffic Separation Scheme at approximately 0500 on 21 August 2017. The CO set sea and anchor detail at 0600 on 21 August 2017 in order to ensure optimal crew rest.

21 August 2017

2. At 0115, the CO reported to the bridge in preparation for the high contact density environment.

3. At 0436, the CO ordered the steering mode to be shifted from computer-assisted manual to back-up manual mode.

4. At 0519, the CO directed the split between steering and thrust control.

5. At 0520, the JSM enters the Singapore Strait Traffic Separation Scheme.

6. At 0521, the Helmsman reports a loss of steering.

7. At 0522, the CO via the Officer of the Deck ordered a reduction in speed from 20kts to 10kts. The Lee Helm only had control of the port shaft, and subsequently only reduced the speed of the port shaft.

8. At 0523, Aft-Steering was manned and manually took control of steering by pressing the emergency override to manual button on the Alternate Steering Control Unit.

9. Right as steering was shifted to Aft-Steering (0523), the Helmsmen on the bridge pressed the emergency override button which now returned steering control to the Helmsman position on the bridge.

10. At 05:23:17, the CO ordered right standard rudder. This is a 15-degree turn.

11. As the CO ordered the rudder command, the steering control had been transferred again to Aft-Steering.

12. At 05:23:28, Aft-Steering had steering control in computer-assisted manual mode.

13. At 05:23:43, the rudder is now right 15 degrees.

14. At 05:23:58, the M/V ALNIC MC impacted the JSM.

C. DEFINING THE SYSTEM(S) AND HAZARDS INVOLVED IN THE LOSS

There were two main physical processes at play in this incident at sea. One physical process is the operation of a U.S. Navy destroyer, and the other being the operation of a civilian merchant vessel. As mentioned previously, the focus of this case study will be the processes that failed on the JSM. The M/V ALNIC MC's inaction was a contributing factor in the collision. Her design space is out of the control of U.S. Navy engineers and therefore the safety control structure will not be detailed in this case study. Figure 4 is a notional safety control structure for JSM.

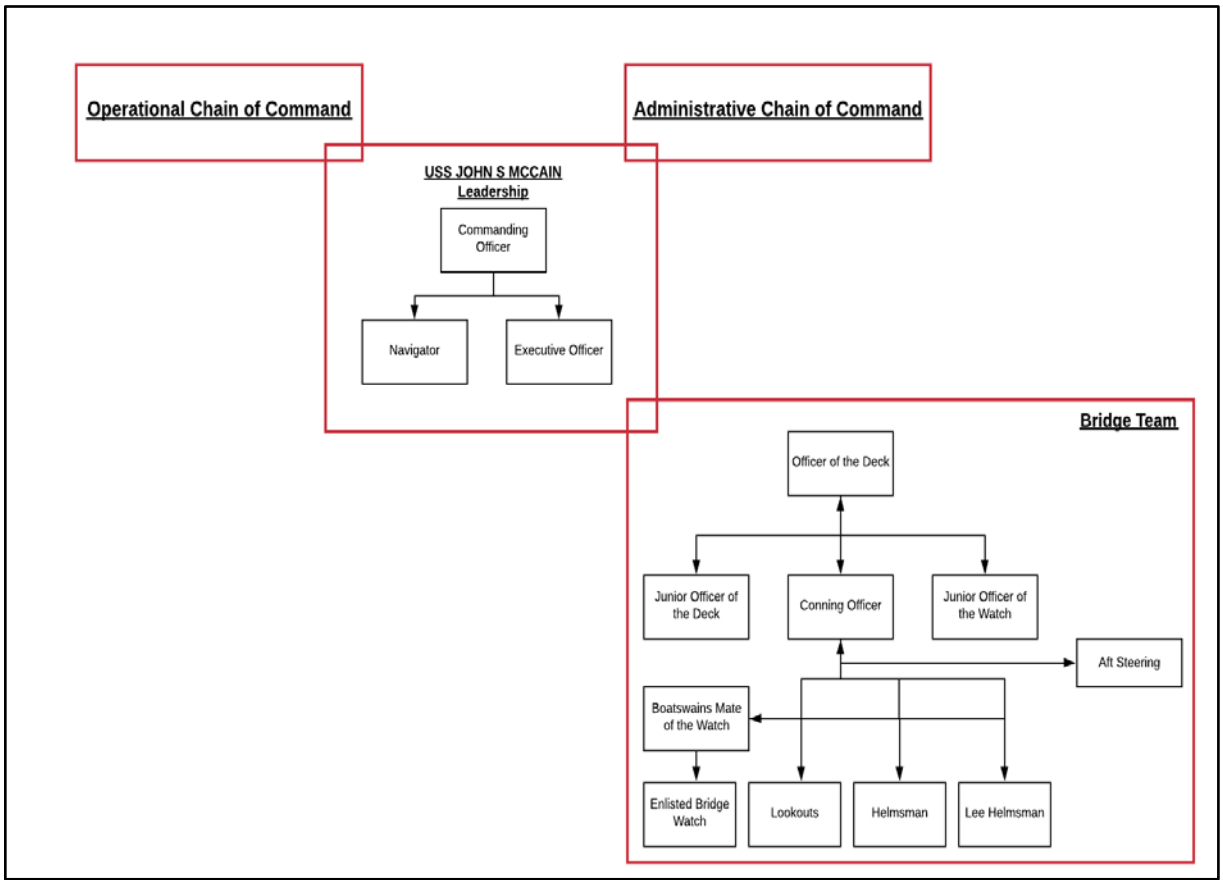


Figure 4. Notional safety control structure for JSM. Adapted from [9].

When operating a U.S. Naval warship at sea, one of the most dangerous hazards is collision at sea. The system-level safety constraints in place to mitigate a collision at sea are:

- Sail in accordance with the Convention on the International Regulations for Preventing Collisions at Sea (COLREGS) [10]
- All members trained in their respective watch positions
- Comply and enforce the Commanding Officers Standing Orders

D. DOCUMENTING THE SAFETY CONTROL STRUCTURE

Now that the system level constraints have been identified, expanding on them provides the specific safety constraints that need to be in place to prevent accidents. Sailing in accordance with COLREGS is pretty straight forward: A vessel either does or does not. The bridge watch team must be well versed in the rules. COLREGS allows all mariners to be on the same page. They provide procedures on how to interact at sea. It does not matter whether it is a military vessel or a civilian vessel. COLREGS must be adhered to.

Each watch position has very specific roles. Referring back to Figure 3, each of those positions carry different qualification standards. For example, the Officer of the Deck, who is in charge of running the bridge watch team will have had to complete several personnel qualification standards and also successfully pass an oral board with the CO. Once deemed a qualified Officer of the Deck, that sailor has the trust and confidence of the CO to safely and professionally sail the vessel at sea. The other bridge team positions do not have that same level of requirements, but that is just because they have fewer responsibilities. Each member of the bridge team will be qualified in their specific role. The Helmsman will have completed the personal qualification standard for the Helmsman position and so on.

Every U.S. Naval warship's CO promulgates Standing Orders. These orders cover just about every standard scenario a U.S. Naval warship will find themselves in. The Standing Orders cover topics such as how close to other vessels you can be before a voice report to the CO is required, or how to position the ship when preparing for flight operations. Every CO has their own set of Standing Orders and hence they will all vary from ship to ship and CO to CO. It is the responsibility of the bridge watch team to be intimately familiar with them.

E. ANALYZING THE PHYSICAL PROCESS

The proximal event chain that leads up to the accident is a great way to hone in on the key actions that contributed to the overall result. The CO had decided to set the sea and anchor detail after the ship would already be in the traffic separation scheme (TSS). The sea and anchor detail is a beefed-up watch team. There are additional watch team members and the personnel assigned are typically the more seasoned watch standers. The times you would set a sea and anchor detail are when the vessel is conducting more complex operations (e.g., pull in/out of port, sailing through high traffic density areas). Planning to man the sea and anchor watchbill mitigated some of the risk associated with traveling through the TSS. That safety constraint failed when the CO determined that he would man the sea and anchor an hour after the JSM entered the TSS.

Prior to entering the TSS, the CO ordered the Helmsman to shift the Steering Control Console (SCC) from computer-assisted manual mode to backup manual mode. There are several modes that the SCC can operate in. The two modes used onboard JSM are computer-assisted manual mode and backup manual mode. The difference between these modes is how the SCC communicates with the rudder control box. In computer-assisted manual mode, the SCC utilizes computers and software to communicate, where backup manual utilizes copper wire. Aside from the operating modes, there are five locations that a watchstander can drive the ship from. See Figure 5 for the layout of the JSM's bridge. There are four stations on the bridge a watchstander can drive the ship from, and one station known as the Aft-Steering Unit (ASU). The ASU is only manned and utilized in an emergency.

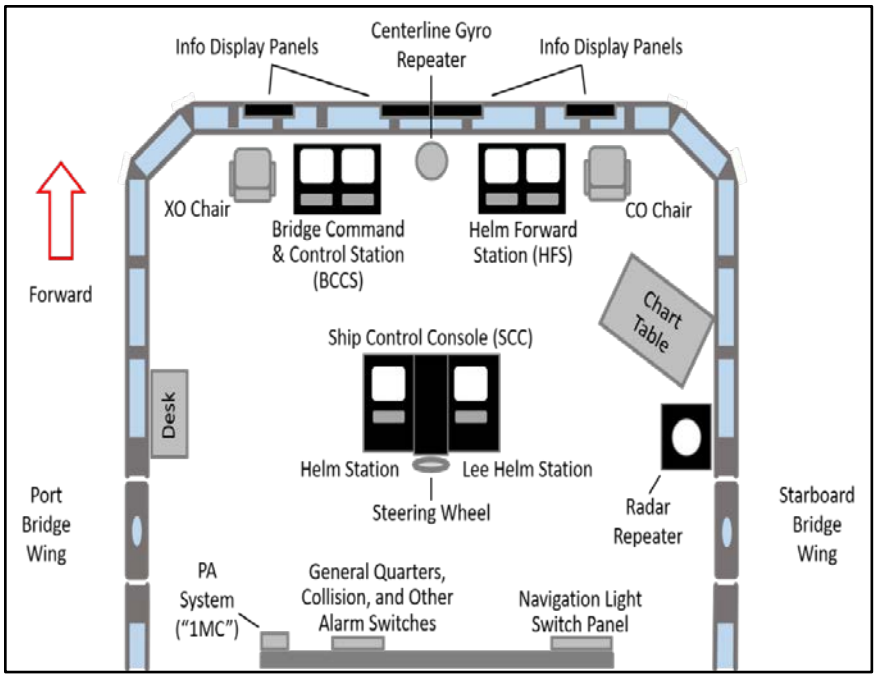


Figure 5. USS *John S. McCain* bridge layout. Source: [6].

According to the Integrated Bridge and Navigation System (IBNS) technical manual, when in backup manual mode, any other station can unilaterally take control of steering. When in computer-assisted manual mode, the transferring of steering requires the relinquishing station to initiate and the gaining station to acknowledge. This represents a safety-constraint by not allowing any station to just take control of steering. However, by the CO ordering the SCC be shifted to backup manual mode, this safety-constraint is no longer in place and steering can be unilaterally taken by any of the five stations.

The CO had good intentions by ordering the splitting of the responsibility of thrust and steering control. Up to this point, the Helmsman was also the Lee Helmsman. Steering and thrust control was all done by one person on one console. In Figure 6 the green shaded portion is the Helm station, and the blueish grey portion is the Lee Helm station.

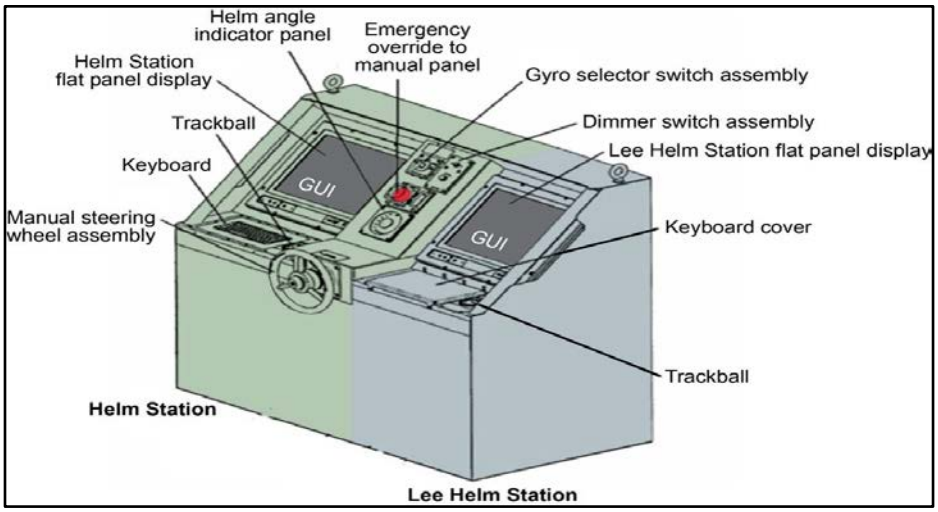


Figure 6. USS *John S. McCain* SCC. Source: [6].

Once a sailor had assumed the Lee Helm position, the sailor began the thrust control transfer from the helm station to the lee helm station. Thrust control transfer is done in a similar fashion as steering control transfer. The one difference for thrust control transfer is that control of each shaft is done one at a time. The JSM is a dual-shaft ship. The relinquishing station (Helm Station) initiated the transfer of the port shaft, and the gaining station (Lee Helm Station) accepted the transfer. At this point, the Lee Helm has control of only the port shaft. Right before the Helmsman initiates the transfer of the starboard shaft, he determines he no longer has control of steering. In line with proper watch standing, the Helmsman announces that he has a loss of steering.

Analysis of video logs that time stamp all transfers and configuration changes revealed that the steering was transferred to the Lee Helm station around the same time that the two stations (Helm and Lee Helm) were conducting the thrust transfer. Figure 7 shows how the SCC displays the current location of steering control and the mode of steering.

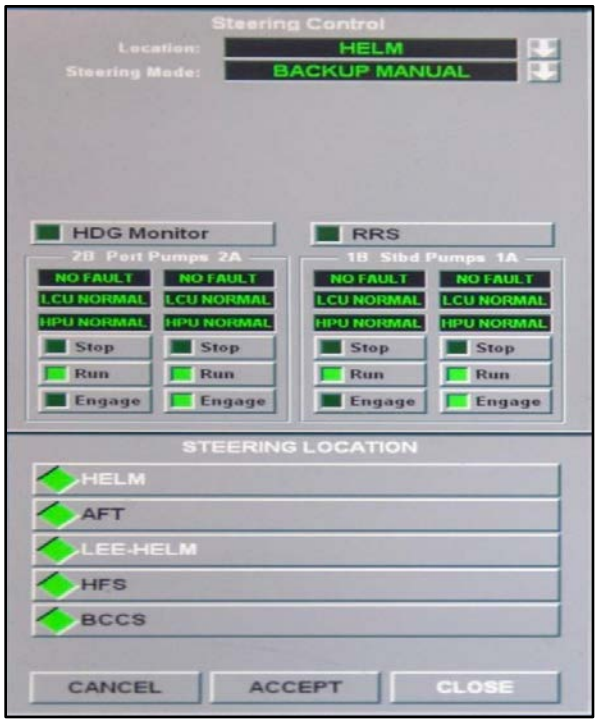


Figure 7. Image of a portion of the IBNS console onboard USS *John S. McCain*. Source: [6].

According to the Helmsman, the steering console will sound an alarm when there is a loss of steering at that station. The alarm notifying the Helmsman of a loss of steering is a safety constraint that can immediately bring the steering loss to the attention of the Helmsman. This is especially helpful if the Helmsman is operating in a more automated mode (i.e., less hands on), which may eliminate the typical haptic feedback one would get if steering control was lost. The video logs show no loss of steering and that it was actually transferred to the Lee Helm station; this raises some concern. Software defects can be challenging to find in complex systems, but the evidence presented in the accident reports makes a strong case for concluding that steering control transfer was done unbeknownst to the Helmsman. Since the SCC was in backup manual mode, the unilateral transfer of steering was possible.

Once the Helmsman announced a loss of steering, the CO ordered a reduction in speed. The JSM had been travelling at 18kts, and the Officer of the Deck ordered the speed be reduced to 10kts. When the initial thrust transfer was conducted the process was

interrupted due to a perceived loss-of-steering event. During the commotion, the Lee Helmsman completed the transfer of the starboard shaft by himself. Prior to the port thrust transfer, when the Helmsman had control of both steering and thrust, the shafts were ganged. The term ganged refers to the control mechanism that is utilized to adjust shaft speed. When the shafts are ganged, any adjustment made to one shaft will also be made automatically on the other. Figure 8 shows what the IBNS thrust control screen looks like.

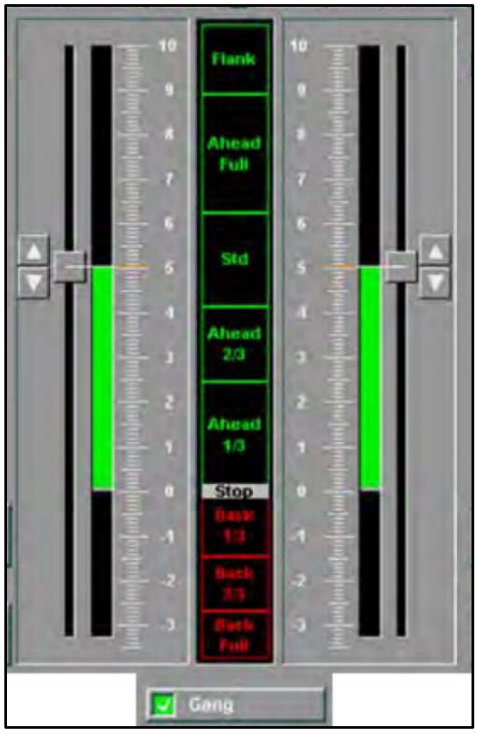


Figure 8. IBNS thrust control GUI. Source: [6].

The Lee Helmsman acknowledged the speed change order, and adjusted the port shaft accordingly in order to achieve the 10kts. The Lee Helmsman had intended to adjust both shafts, but the shafts became un-ganged and the Lee Helmsman was unaware of this when he adjusted the speed. The Lee Helmsman told the NTSB investigator that he had re-ganged the shafts after the transfer. Since only one shaft's speed was adjusted, the ship started to drift to port. The slower speed on the port shaft and the faster speed on the starboard shaft essentially put JSM into a port-twist. When transferring thrust from one

station to another, the settings at the previous station should travel with the control. A safety constraint should have existed here, and the un-ganging of the shafts should not have happened.

The Aft Steering Unit (ASU) now manned after the bridge watch team called away the loss of steering at the helm station on the bridge. When there is a loss of steering on the bridge, the secondary control point is the ASU. The CO ordered the ASU to take control of steering, and the ASU acknowledged the order and pressed the emergency-override-to-manual button. See Figure 5 for reference. By pressing the emergency-override-to-manual button, that station will unilaterally take steering control and the mode of steering will shift to backup manual. The watchstander at the Helm Station believed that in order for the ASU to take control, he needed to hit the emergency-override-to-manual button at his station. A few moments go by, and the Helmsman on the bridge realizes he has positive steering control (i.e., physical control of steering has been regained). Positive steering control at the SCC is announced. The CO orders a “right 15 degrees rudder” and reducing the speed to 5kts. The video logs show that both shafts were adjusted to achieve the 5kts. This also corrected the speed difference between shafts from before.

When positive steering control was achieved on the bridge at the SCC, the ASU requested to take back control of steering and the Helmsman at the SCC granted the request and relinquished control of steering back to the ASU. The CO had ordered a 15-degree rudder angle to the right in order to avoid collision with the M/V ALNIC MC, but when the steering was shifted back to the ASU for the last time the rudders swung a minimum 15-degrees to the left. The ASU dialed up the 15-degrees to the right rudder angle, but this control action was too late. The JSM and M/V ALNIC MC collided at 05:23:58. There was confusion amongst the watchstanders about how the IBNS functions as modes change and the locations of steering changed. System complexity overcame the watch team. This was a root cause for the collision.

F. ANALYZING THE HIGHER LEVELS OF THE SAFETY CONTROL STRUCTURE

Referring back to Figure 3, the Bridge Team is the operational level of this process. The CO, XO, and Navigator make up the leadership triad from a seamanship and navigation perspective onboard the JSM. The ship has an operational chain of command and an administrative chain of command. Since the JSM was stationed in Yokosuka, Japan, she operationally falls under Commander, SEVENTH Fleet (C7F) who then reports to Commander, U.S. Pacific Fleet (COMPACFLT) in Honolulu, HI. COMPACFLT operationally reports to the Commander, U.S. Indo-Pacific Command (USINDOPACOM). COMPACFLT is USINDOPACOM's Naval Component Commander and is responsible for providing USINDOPACOM ready naval assets.

The administrative chain of command is similar to the operational but deviates at COMPACFLT and includes Commander, Naval Surface Forces Pacific (COMNAVSURFPAC). COMNAVSURFPAC is responsible for the manning, training, and equipping of the surface forces in the Pacific theater. Analyzing the higher levels of the safety control structure for this accident will mostly involve the administrative chain of command due to the manning, training, and equipping of JSM being identified as the root issues.

The U.S. Navy's answer on how to streamline processes on the bridge was to introduce automation implemented via software that can handle multiple legacy system functions. With shrinking budgets, the IBNS was supposed to make navigating the world's oceans less complex and less manning-intensive. There was clear evidence of operator error onboard JSM, but a series of decisions made at the higher levels also contributed to the environment that allowed these errors to happen in the first place. A requirement existed to have an IBNS specialized technician onboard, but due to staffing shortages the higher-levels waived the requirement [11]. Gaps in documentation of IBNS were discovered during the investigation period, notably JSM's IBNS documentation onboard was said to be three years out of date [11].

The higher levels in the safety control structure are critical in the U.S. Navy. As with most hierarchical structures, the lower levels depend on the higher levels to function

correctly. The Comprehensive Review of Recent Surface Force Incidents noted that, "There were decisions at headquarters that stemmed from a culturally engrained 'can do' attitude and an unrecognized accumulation of risk that resulted in the ships not being ready to safely operate at sea" [8]. While this case study does not go into the details of U.S. Navy culture, the point being made is saying "no" or "I don't think we can handle that" is not part of the vocabulary. When given a task, a sailor (all levels) will do it to the best of their ability and will just find a way to get it done. This accident has put a spotlight on the surface forces, and while tragic due to the loss of life, a certain level of reflection appears to have taken place amongst the force. The Comprehensive Review of Recent Surface Force Incidents went into great detail of the history of the integrated bridge system concept and lays out a very respectable plan on how to approach the future of bridge modernization. A key comment made in the review which encompasses exactly how the U.S. Navy should integrate complex technology not only on the bridge of warships but through all safety-critical systems.

> For safety critical controls interfaces, issues like these should be prevented through upfront analysis of human-machine-interface requirements and validated through qualification testing in advance of equipment delivery. If thorough human factors assessments, land-based testing, and design qualification are considered too expensive or time consuming, then modernization of these controls systems should not be undertaken [8].

G. COORDINATION AND COMMUNICATION

Communication failures can be found in almost all accidents. The bridge watchteam on board the JSM did not communicate effectively. From the documents available for analysis, the internal communication was mediocre at best, but it is the external communications that led to a higher-risk state. The CO ordered the navigation lights be adjusted to represent the ships current status as they combat the perceived loss steering casualty. This notifies mariners in the surrounding area that the vessel is unable to maneuver in accordance with the COLREGS. The investigation revealed the navigation lights were never adjusted prior to the collision. Additionally, the Bridge-to-Bridge (BTB) radio is used to communicate with vessels in the surrounding area. Under nominal operations the BTB is used to coordinate things from safe distance passing to notifications

of special operations the vessel may be conducting. The accident reports revealed that the officer of the deck (OOD) did not make contact with the M/V ALNIC MC. Had the Master onboard M/V ALNIC MC been more aware of the JSM's challenges, the Master could have executed precautionary maneuvers to remain a safe distance from the JSM.

H. DYNAMICS AND MIGRATION TO A HIGH-RISK STATE

This has been discussed at length already, but the CO's decision to operate IBNS in backup manual mode instantly put the ship in a high-risk state. The added protection designed into the other modes of operation were not ignored but not understood. The general consensus from reviewing the documents pertinent to the accident is that the unilateral transfers of steering and thrust in backup manual mode was unknown. Additionally, during the initial investigation, the CO made it very clear that he had little confidence in the IBNS. His decision to execute a thrust transfer to an alternate control station while in the Singapore Strait TSS added to the complexity of the current state.

I. RECOMMENDATIONS AND FINDINGS

The use of STAMP to conduct this survey level accident analysis did not result in the uncovering of any previously undocumented findings. The use of STAMP does provide a very clear and concise process on how to approach the analysis of accidents involving complex systems. This analysis relied heavily on the three documents mentioned in the introduction, and each document seemed to be geared towards different audiences. By utilizing the STAMP method, all three documents can be captured in just one. That is not necessarily an undiscovered finding, but something to keep in mind.

The recommendations from the reports are broad and leave room for the technical experts to interpret. Shortly after the collision, there have been "class advisories" published to bring key weaknesses of the system to the attention of units that have IBNS. The Navy has decided to stick with the IBNS system, but is in the process of re-introducing the physical throttles that control speed of each shaft [12]. The investigation found that IBNS was not to be compliant with ASTM International in Standard F1166, *Standard Practice for Human Engineering Design for Marine Systems, Equipment, and Facilities.* The implementation of a control mechanism that measures a discrete value vs. a continuous value

is the subject of non-compliance. It is noted that touch-screen controls are not appropriate for continuous control functions. The throttle control falls into this category. The non-compliance is probably driving the quick reaction by Naval engineers to re-introduce the physical throttles to the bridge.

One recommendation that seems appropriate is a deeper look at safety constraints in place when operating in backup manual mode. The initial design scheme allows the unilateral transfer to any station which can be useful in the event there is a casualty and only one station is accessible. That scenario is still valid, and that functionality should remain, but there can be another layer that requires the user to acknowledge the unilateral request. This could be a simple software modification that would add a safety-constraint in backup manual mode.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONTEXT AWARENESS IN SAFETY CRITICAL SYSTEMS

A. WHAT IS CONTEXT AWARENESS?

Before understanding what a Context-Aware System is, we must define the terms context and awareness. The Merriam-Webster Dictionary definition of context is (1) "the parts of a discourse that surrounds a word or passage and can throw light on its meaning" [13], (2) "the interrelated conditions in which something exists or occurs" [13], and the definition of awareness is (1) "knowledge and understanding that something is happening or exists" [14]. The second definition of context is the one we care about. Now take the term context-aware; the knowledge and understanding of interrelated conditions that exists or occurs. As humans, this is a basic everyday function. During any given day, humans find themselves in many different situations that require a degree of awareness and some level of understanding the context of the situation. Many of these situations involve human-to-human interactions, and how a human navigates the situation can determine characteristics about him or her. This is more of a social approach to understanding context awareness. We are interested in understanding context-aware computing, and you will find that the underlying themes are the same.

Thinking about our human example, how could systems behave in a similar manner? It is definitely a new way of thinking about computing. From the beginning of personal computing to modern day, a computer was considered a 'dumb' machine. A user (human) would instruct the machine to perform an operation and the machine would follow those instructions precisely. If the human instructions were erroneous or flawed in any way, the computer would fail at correctly performing the operation. The machine had no way to determine whether the input it receives from the human is correct or what the human intended for a particular context of performing work. Imagine the everyday convenience humans could experience if computers had the ability to understand and adapt to their environment and the user they are interacting with. "One hypothesis that a number of ubiquitous computing researchers share is that enabling devices and applications to automatically adapt to changes in their surrounding physical and electronic environments will lead to an enhancement of the user experience" [15].

In 1994 M. Theimer and B. Schilit introduced this idea of context-aware computing [16]. They defined context-aware computing as "the ability of a mobile user's applications to discover and react to changes in the environment they are situated in" [16]. Their definition is somewhat constraining: There is no reason that context-awareness should be limited to mobile applications. This idea of context-aware computing has been applied over a mired of applications; tourism, the retail market, transportation, event planning, and healthcare to name a few [16]. Figure 9 provides a visual aid of a basic context-aware system.

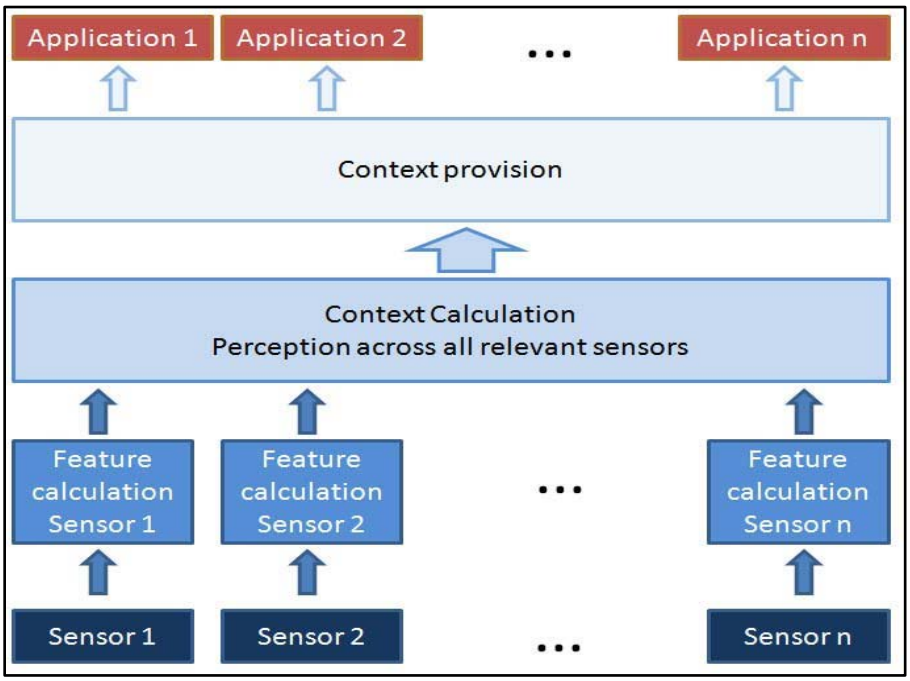


Figure 9. Example of a basic context-aware computing system. Source: [17].

B. SHIP STEERING, NAVIGATION, AND COMPLEX TECHNOLOGY

When one thinks about all the important or critical systems that make up a U.S. Naval warship, the first thoughts are typically about big guns or missile systems. Those thoughts are not wrong. The weapon systems onboard U.S. Naval warships are absolutely critical, but what about the system that maneuvers and guides the warship? The steering and navigation system is arguably just as critical as a weapon system. If you cannot sail the seas and confront your enemy, how will you ever deploy your weapon systems?

The fundamentals of steering a ship have been largely unchanged from the days of sail. The ship has one or more rudders and some way of moving the rudder in the desired direction so that the flow of water will be deflected, resulting in the stern moving away from the direction the rudder is pointing. Whether this be a steering oar, a rope and pulley system, steam generated mechanisms, or electro-hydraulic systems the result is typically the same [18]. The rudder moves in the direction it was commanded. As ships grew larger and became faster, the means of moving the rudder also changed. The torque required and the speed at which it moved needed to keep up with the demands of the vessel it was steering [18]. While the mechanical engineering behind these more modern steering systems is complex, the designs are tried and true. A probability of failure in the mechanical components of a modern steering system is very low. However, maintaining acceptable levels of reliability and safety continue to be challenging as the complexity of steering systems increase and increasing percentage of steering functionality is allocated to software.

Despite its complexity, automation via software of the steering function frees the mariner to perform other important tasks. However, automation of safety-critical functions like steering does not always have the intended outcome, as evidenced by the mishap experienced by the USS *John S. McCain*. While the complexity of the new Integrated Bridge and Navigation System played a role, the human-computer interface seems to be the central safety issue. In reference to the retrofitting of the physical throttle controls, U.S. Navy sailors preferred the less complex configuration, and it was the overwhelming sentiment that the less complex the system the more reliable it was [19].

The Integrated Bridge and Navigation system is far more complex then legacy steering systems, but nowhere near as complex as a system incorporating technology such as artificial intelligence. In addition, military commanders are held accountable for their own actions and the actions of every individual under their command. In such a culture in which critical decisions can cost careers and in worst-case scenarios lives, how do we engineer such systems so that users will accept delegation of machine making critical decisions? That all being said, the Department of Defense knows the direction it must head.

> The U.S. Department of Defense (DOD) protects our nation by deterring war and winning the nation's wars when deterrence fails. In fulfilling this mission, we have always been at the forefront of technological advances to ensure an enduring competitive military advantage against those who threaten our security and safety. Artificial Intelligence (AI) is one such technological advance. AI refers to the ability of machines to perform tasks that normally require human intelligence - for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action - whether digitally or as the smart software behind autonomous physical systems [20].

Can the implementation of artificial intelligence in DOD safety-critical systems increase safety and reliability in a way that sailors will trust the machine to do all the right things when employed? The ethical challenges that artificial intelligence poses have little to no impact on a steering system. That makes this scenario slightly less complex when evaluating the sociotechnical aspects of incorporating this kind of technology. AI does make the system more technically complex, but does the sailor need to understand or be able to explain every aspect of the system and the decisions it makes?

The scope of systems the DOD utilizes is quite broad, systems that make decisions on when ordnance should be fired will require a higher level of explainability than other systems that pose lesser risk of harm. There are a handful of flavors of AI, and fully autonomous, which most think of when AI is mentioned, is not always the answer. In DOD safety-critical systems it is almost never the answer. That is true now but as technology advances and a culture shift occurs that may become less true.

Human-in-the-loop, human-out-of-the-loop, and human-on-the-loop are the flavors of AI systems that could be viable options for DOD safety-critical systems [21]. As mentioned above, human-out-of-the-loop is farther in the future, but human-in-the-loop AI implemented into a steering system could be a game changer. On the bridge of U.S. Navy warships every single watchstander is familiar with two concepts: Bridge Resource Management (BRM) and watchteam back-up. BRM is a method of utilizing all of your available resources during operations. Operating in a vacuum is never the answer. Spreading the load during times of intense data flow is guaranteed to make any operation safer and more efficient [22]. Watchteam back-up is a similar concept but just a bit less

formal. Everybody on the bridge has set roles and responsibilities, but everybody should have a level of situational awareness that can assist the watchteam where necessary.

The future steering and navigation systems could implement some form of context awareness that would act as an additional layer of watchteam backup or BRM. This concept being a human-in-the-loop system would not take away decision-making abilities, but rather serve as a decision-shaping tool. In addition to the other bridge watchstanders, this new system would process all relevant data being fed to it and output decision-shaping recommendations to aid the human watchstander in the execution of watch-standing duties.

C. A HYPOTHETICAL CONTEXT AWARE LAYER IN THE INTEGRATED BRIDGE NAVIGATION SYSTEM

There were two significant events that took place onboard JSM leading up to the collision that this new theoretical system could have aided in preventing:

1. The unintended transfer of steering from the helm station to the lee helm station.

2. The un-ganging of shafts during thrust transfer from the helm station to the lee helm station.

A system being aware through the sensing of conditions, such as the environmental context and system state could aid in mapping to hazards. The human-machine partnering is paramount here. IBNS did not alert the Helmsman nor Lee Helmsman about the potential of their control actions to move the ship into an unsafe state. The context-aware system would detect such behavior and provide an alert in the form of a warning. If desired (and acceptable to the users) the system could take some level of active control, such as trying to return steering control to the location it was unilaterally taken from.

Figure 10 and 11 provide a visual depiction of the two actions that the Helmsman and Lee Helmsman took and will provide a simpler way to conceptualize the system weaknesses. Followed by Figure 12, which is the same actions but with a theoretical context-aware layer introduced.

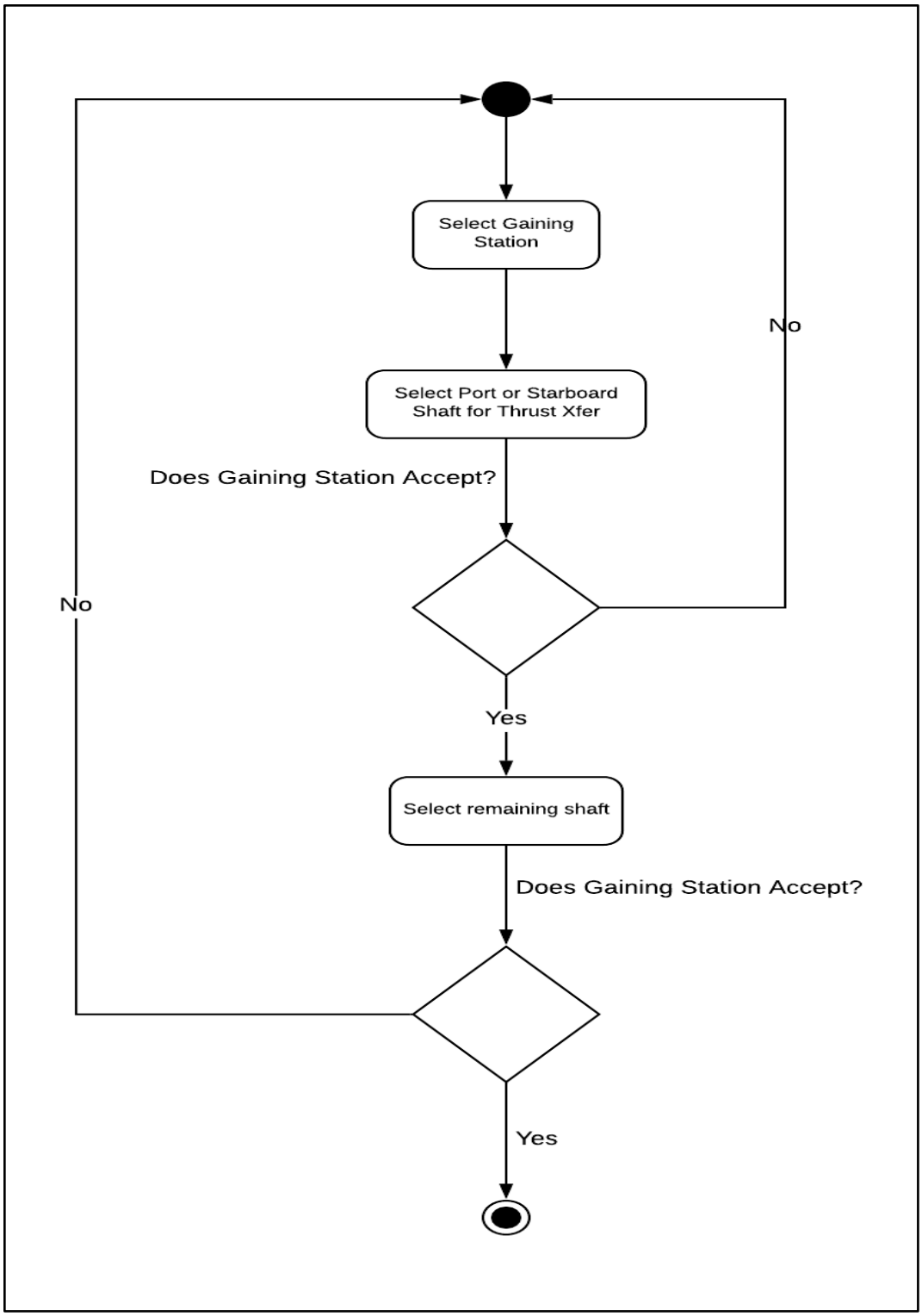


Figure 10. Control actions taken to transfer thrust in computer-assisted manual mode.

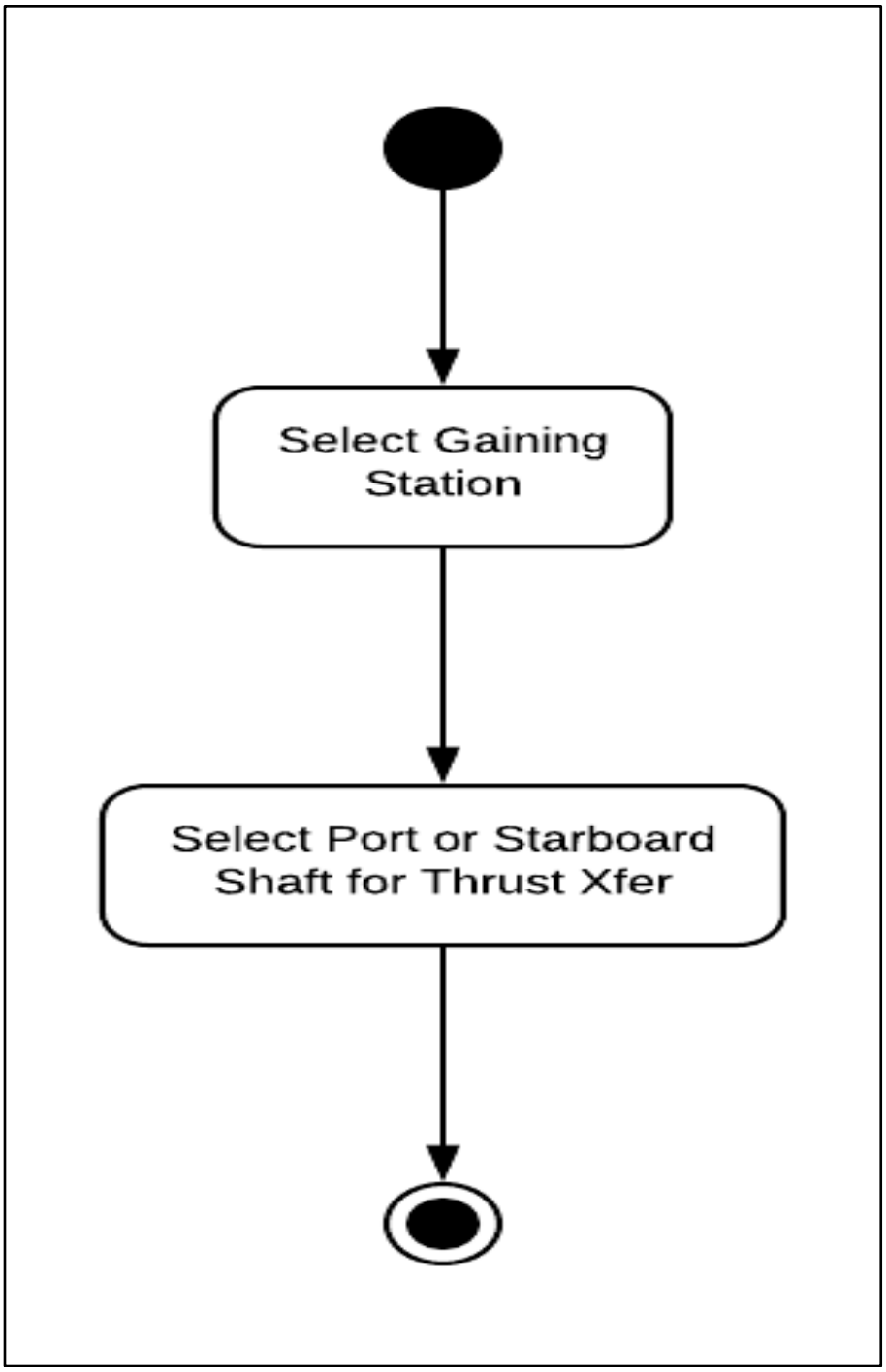


Figure 11. Control actions taken to transfer thrust in backup manual mode.

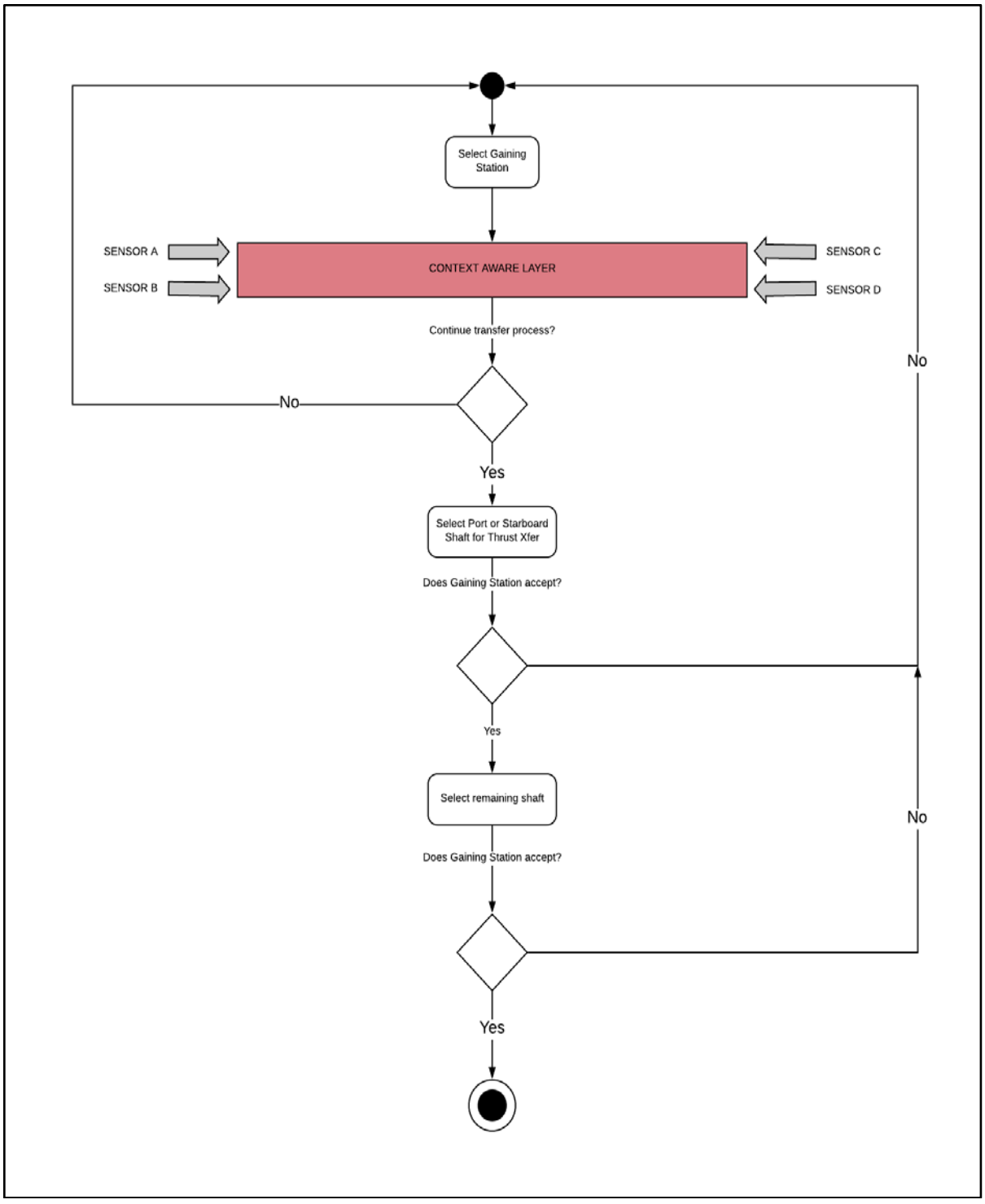


Figure 12. Control actions taken to transfer thrust with context-aware layer.

Figures 9 and 10 show the control actions required for thrust control transfer in both computer-assisted manual mode as well as backup manual mode. It is quite clear that thrust transfer in backup manual mode has significantly less safety-control measures in place. The most significant safety-control measure in place when operating in computer-assisted manual mode is that the transfer must be initiated by the station that currently has thrust control, and acknowledged by the station that is gaining. This process will be completed twice, once per shaft.

This same task but with a context-aware layer could be instrumental in creating a safer execution of such operations in all available modes. Figure 11 has an added layer of context-awareness directly after the first control action. The context-aware layer here relies on an array of sensors to provide the human operator with information about the operating environment. The integration into the bridge and navigation system would utilize key sensor feeds from sources such as navigation, RADAR, and system status.

The navigation data would provide the system with situational awareness of the navigational scheme the ship is operating in. The way a ship operates in the open ocean is different than when piloting. The RADAR data would provide the system a 360-degree contact picture. While traditionally the helm and/or lee helm positions do not play a role in contact management, a context aware bridge and navigation system would enable them to become part of that process. The more eyes the better when trying to manage a dense contact picture. This also directly ties into the BRM concept discussed previously. A system status data feed would provide key elements of the critical systems involved with surface vessels: which engines are online, where is steering located, where is thrust control located, are throttles ganged, overall health of these components, etc.

Onboard JSM, the unintentional transfer of steering during the thrust transfer was a consequence of a poorly designed user interface among other things. This context aware layer would have questioned this transfer. A unilateral transfer of steering initiated by the lee helm position while all system indicators present no steering system casualty at the helm station would initiate some form of behavior-shaping mechanism. Additionally, a shift in location of steering in a dense contact environment such as the Singapore Strait is

not a common procedure when no steering casualty is present. This uncommon action would be another red flag used by the system to generate behavior-shaping mechanisms.

During the thrust transfer from the helm station to the lee helm station the throttles became unganged. A context-aware layer may not have ensured the ganged function traveled during the transfer process, but the layer would have questioned the actions of the lee helm once speed changes were made. A split-shaft throttle maneuver is for the most part reserved for piloting waters and pier-side maneuvers. When operating in the open ocean environment, there is almost never a need to have one shaft set at a different speed than the other. When the Lee Helm reduced speed on JSM, only one shaft speed was reduced. The context-aware system would have questioned this action as it would be flagged as non-typical for the current operating environment. By immediately bringing this to the watchstanders attention he or she could re-gang the throttles and continue operations unaffected.

One possible way the contextual information could be provided is through distributed real-time augmented reality. This could provide multiple views of the situation to the helmsman and others, that is, overlays of information on a virtual reality. A heads-up display that can be configured to provide these watchstanders all relevant information to the performance of their duties would greatly enhance their visual understanding of the environment and the physical status of the systems they control.

One of the potential unintended consequences is that the system may undo an action that it thinks is hazardous and could lead to an unsafe state when in fact the sailors on the bridge are actually making the intended action. In terms of cars, this would be like having a vehicle with an intelligent lane-keeping system, that is, a control system for automated steering (known as lateral control). Suppose a toy ball, followed by a child, rolls out in front of the car and the driver tries to swerve to miss the child and toy. The intelligent steering system tries to keep the car in the lane. These are conflicting decisions and control actions. The system can only reason with the data it receives from sensors and decision rules (algorithms) it has been programmed to process.

This concept would require no additional training beyond what is already required. Understanding the complexity of how the data flows and is processed is not vital to the watchstanders. The behavior shaping recommendations/mechanisms do not require any action by the watchstander, and can be ignored if the actions taken by the watchstanders are in fact correct. The overwhelming majority of sailors are smart, attentive, and overly qualified in the positions they man. Trusting such a system is no different than trusting your fellow watchstanders. In the example of the USS *John S. McCain* mishap, a context-aware system would have most likely proved to increase the safety of that scenario. A thorough causal factor analysis would go much deeper than these surface-level discoveries, but there is no real way of getting around the fact that these two missteps by the watchstanders were significant hazard causal factors. Had they received local, instantaneous notification/recommendations based on their input orders, the outcome might have been different.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FUTURE WORK AND CONCLUSION

The realm of artificial intelligence implemented into safety-critical systems is fairly new and has unlimited room to grow. The context-awareness capabilities discussed here are not meant to replace the human user, but to enhance the safety and effectiveness of the IBNS and other systems used on U.S. Navy ships. This study scratched the surface, leaving plenty of avenues for future work such as:

1. Developing a prototype of a context-aware IBNS.

2. Collaborating with Naval Ordnance Safety and Security Activity (NOSSA) to incorporate the approach used in this study into the Navy's system safety engineering practices.

3. Investigate how the introduction of context-awareness capabilities may themselves introduce safety hazards.

The ever-increasing complexity of technology has introduced new challenges that safety professionals must confront. Long gone are the days in which classical safety engineering techniques alone are effective [3]. This study demonstrated that the STAMP method helps the safety engineer identify safety hazards and causal factors throughout a system's control hierarchy. "What they lacked, and what we have been hindered in our progress by not having, is a more powerful accident causality model that matches today's new technology and social drivers" [3]. The study also demonstrated how the application of STAMP can be used to identify where in a system safety hazards associated with human-machine teaming can be addressed by improving through the introduction of context-aware capabilities.

The demand signal for more advanced technology that can enable the warfighter to better perform their duties grows stronger every day. The Department of Defense and Department of the Navy have published high-level doctrine in the past two years demonstrating the seriousness of their commitment to the adoption of AI. There has been little work done on applying this doctrine to actual cases though. This study which suggests

the benefits that a context-aware system could provide was mindful of the ethical principles of artificial intelligence that the DOD has recently adopted. The principles cover five areas that are critical to producing effective and safe artificial intelligence [23]:

1. Responsible. DOD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
2. Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.
3. Traceable. The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
4. Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.
5. Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior. [23]

The human-in-the-loop AI being suggested in this study must be reliable and governable above all else. How the system is designed, maintained, and analyzed will be critical to ensure it meets the standards of these principles. Nancy Leveson's STAMP method can be the DOD's solution. Developing a system from the ground up with STAMP is a commitment to safety, and with the complexity of future systems on the rise, safety should be at the forefront of every engineer's mind, but at a minimum the safety engineer on an integrated project team needs to be the advocate for safety. "A life without adventure is likely to be unsatisfying, but a life in which adventure is allowed to take any form is sure to be short" [3].

APPENDIX. REPORT ON THE COLLISION BETWEEN USS JOHN S MCCAIN (DDG-56) AND MOTOR VESSEL ALNIC MC

The following is from [6].

1. EXECUTIVE SUMMARY - USS JOHN S MCCAIN

1.1 Introduction

USS JOHN S MCCAIN collided with Motor Vessel ALNIC MC on 21 August 2017 in the Straits of Singapore.

JOHN S MCAIN is a Flight 1 Arleigh Burke Class Destroyer, commissioned in 1994 and homeported in Yokosuka, Japan, as part of the Forward Deployed Naval Forces and Carrier Strike Group FIVE. Approximately 300 sailors serve aboard MCCAIN. MCCAIN is 505 feet in length and carries a gross tonnage of approximately 9,000 tons.

ALNIC MC is a Liberia flagged oil and chemical tanker built in 2008. ALNIC MC is approximately 600 feet long and has a gross tonnage of approximately 30,000 tons.

The collision between JOHN S MCCAIN and ALNIC resulted in the deaths of 10 U.S. Sailors due to impact with MCCAIN's berthing compartments, located below the waterline of the ship. ALNIC suffered no fatalities. U.S. Sailor fatalities were:

ETC Charles Nathan Findley of Amazonian, Missouri, 31 years old.

ICC Abraham Lopez of El Paso, Texas, 39 years old.

ET1 Kevin Sayer Bushell of Gaithersburg, Maryland, 26 years old.

ET1 Jacob Daniel Drake of Cable, Ohio, 21 years old.

ITl Timothy Thomas Eckels Jr. of Baltimore, Maryland, 23 years old.

ITl Corey George Ingram of Poughkeepsie, New York, 28 years old.

ET2 Dustin Louis Doyon of Suffield, Connecticut, 26 years old.

ET2 John Henry Hoagland III of Killeen, Texas, 20 years old.

IC2 Logan Stephen Palmer of Harristown, Illinois, 23 years old.

ET2 Kenneth Aaron Smith of Cherry Hill, New Jersey, 22 years old.

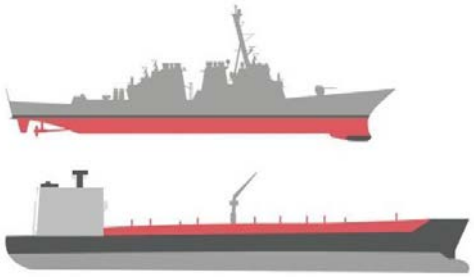
1.2 Summary of Findings

The Navy determined the following causes of the collision:

Loss of situational awareness in response to mistakes in the operation of the JOHN S MCCAIN's steering and propulsion system, while in the presence of a high density of maritime traffic.

Failure to follow the International Nautical Rules of the Road, a system of rules to govern the maneuvering of vessels when risk of collision is present.

Watchstanders operating the JOHN S MCCAIN's steering and propulsion systems had insufficient proficiency and knowledge of the systems.



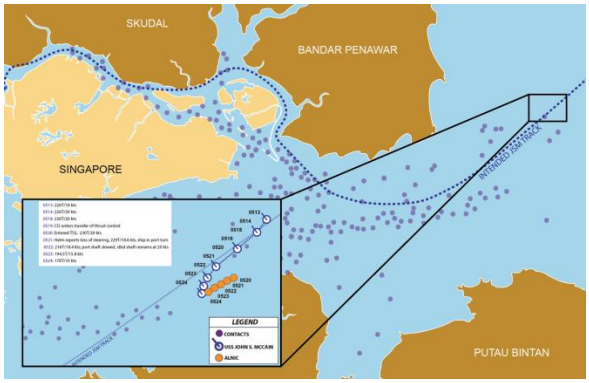


Figure 1 – Relative size of USS JOHN S MCCAIN Figure 2 – Illustration Map of Approximate Collision Location

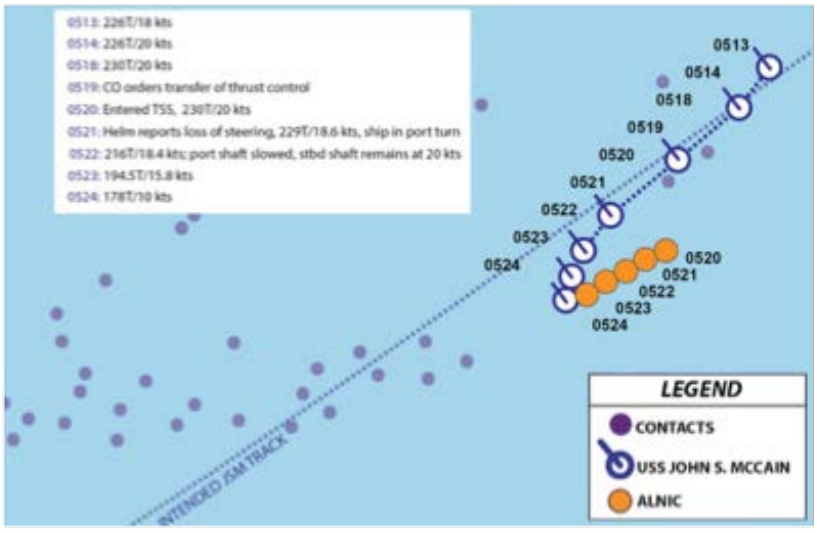


Figure 3 – Illustration Map of Approximate Collision Location

2. DESCRIPTION OF EVENTS

2.1 Background

JOHN S MCCAIN departed its homeport of Yokosuka, Japan on 26 May 2017 for a scheduled six month deployment in the Western Pacific, which at the time of the collision had included operations in the East and South China Seas, and port visits in Vietnam, Australia, Philippines and Japan. On the morning of 21 August, JOHN S MCCAIN was 50 nautical miles east of Singapore, approaching the Singapore Strait and Strait of Malacca, in transit to a scheduled port of call at Changi Naval Base, Singapore. These Straits form a combined ocean passage that is one of the busiest shipping lanes in the world, with more than 200 vessels passing through the straits each day. JOHN S MCCAIN was transiting through the southern end of the Strait. See Figure 2. In the predawn hours of 21 August 2017, the moon had set and the skies were overcast. There was no illumination and the sun would not rise until 0658. Seas were calm, with one to three foot swells. All navigation and propulsion equipment was operating properly.

At 0418, JOHN S MCCAIN transitioned to a Modified Navigation Detail due to approaching within 10 nautical miles from shoal water. This detail is used by the Navy when in proximity of water too shallow to safely navigate as occurs when entering ports. This detail supplemented the on watch team with a Navigation Evaluator and Shipping Officer, providing additional personnel and resources in the duties of Navigation and management of the ship's relative position to other vessels.

JOHN S MCCAIN was scheduled to enter the Singapore Strait Traffic Separation Scheme less than an hour later. Traffic separation schemes are established by local authorities in approaches to ports throughout the world to provide ships assistance in separating their movements when transiting to and from ports. The Commanding Officer had been physically present on the bridge since 0115, a practice common for operations with higher risk, such as navigating in the presence of busy maritime traffic at night. The Executive Officer (XO) reported to the bridge at 0430 to provide additional supervision and oversight to enter port. Although JOHN S MCCAIN entered the Middle Channel of the Singapore Strait (a high traffic density area) at 0520, the Sea and Anchor Detail, a team the Navy uses for transiting narrower channels to enter port, was not scheduled to be stationed until 0600. This Detail provides additional personnel with specialized navigation and ship handling qualifications.

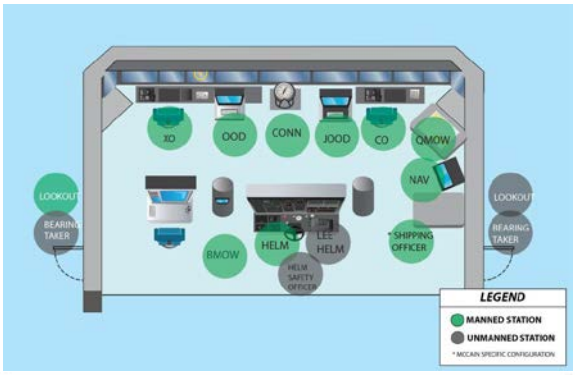
JOHN S MCCAIN was operating by procedures established for U.S. Navy surface ships when operating at sea before sunrise, including being at "darkened ship." "Darkened Ship" means that all exterior lighting was off except for the navigation lights that provide identification to other vessels, and all interior lighting was switched to red instead of white to facilitate crew rest. The ship was in a physical posture known as "Modified ZEBRA," meaning that all doors inside the ship, and all hatches, which are openings located on the floor between decks, at the main deck and below were shut to help secure the boundaries between different areas of the ship in case of flooding or fire.

Watertight scuttles on the hatches (smaller circular openings that can be opened or closed independently of the hatch) were left open in order to allow easy transit between spaces.

2.2 Events Leading to the Collision

At 0519, the Commanding Officer noticed the Helmsman (the watchstander steering the ship) having difficulty maintaining course while also adjusting the throttles for speed control. In response, he ordered the watch team to divide the duties of steering and throttles, maintaining course control with the Helmsman while shifting speed control to another watchstander known as the Lee Helm station, who sat directly next to the Helmsman at the panel to control these two functions, known as the Ship's Control Console. See Figures 3 and 4. This unplanned shift caused confusion in the watch team, and inadvertently led to steering control transferring to the Lee Helm Station without the knowledge of the watch team. The CO had only ordered speed control shifted. Because he did not know that steering had been transferred to the Lee Helm, the Helmsman perceived a loss of steering.

Figure 4 – Bridge Schematic of JOHN S MCCAIN



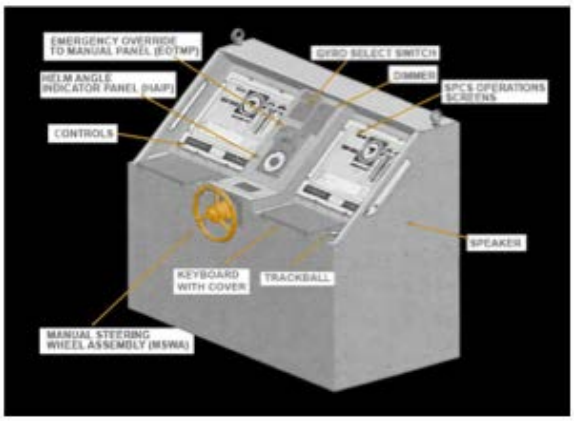


Figure 5 - Illustration of Ship Control Console on JOHN S MCCAIN

Steering was never physically lost. Rather, it had been shifted to a different control station and watchstanders failed to recognize this configuration. Complicating

this, the steering control transfer to the Lee Helm caused the rudder to go amidships (centerline). Since the Helmsman had been steering 1–4 degrees of right rudder to maintain course before the transfer, the amidships rudder deviated the ship's course to the left.

Additionally, when the Helmsman reported loss of steering, the Commanding Officer slowed the ship to 10 knots and eventually to 5 knots, but the Lee Helmsman reduced only the speed of the port shaft as the throttles were not coupled together (ganged). The starboard shaft continued at 20 knots for another 68 seconds before the Lee Helmsman reduced its speed. The combination of the wrong rudder direction, and the two shafts working opposite to one another in this fashion caused an un-commanded turn to the left (port) into the heavily congested traffic area in close proximity to three ships, including the ALNIC. See Figure 5.

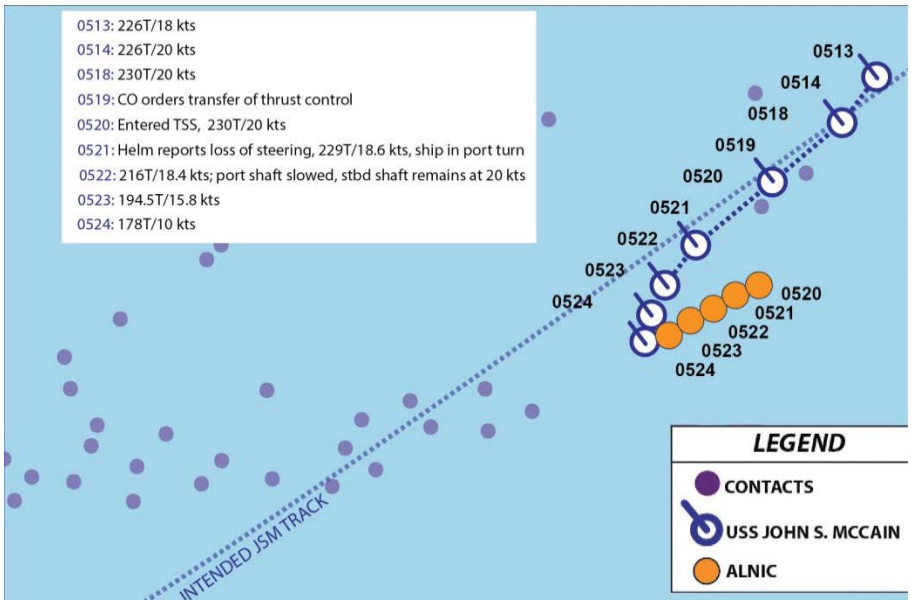


Figure 6 – Illustration Map of Approximate Collision Location

Although JOHN S MCCAIN was now on a course to collide with ALNIC, the Commanding Officer and others on the ship's bridge lost situational awareness. No one on the bridge clearly understood the forces acting on the ship, nor did they understand the ALNIC's course and speed relative to JOHN S MCCAIN during the confusion.

Approximately three minutes after the reported loss of steering, JOHN S MCCAIN regained positive steering control at another control station, known as Aft Steering, and the Lee Helm gained control of both throttles for speed and corrected the mismatch between the port and starboard shafts. These actions were too late, and at approximately 0524 JOHN S MCCAIN crossed in front of ALNIC's bow and collided. See Figure 6.

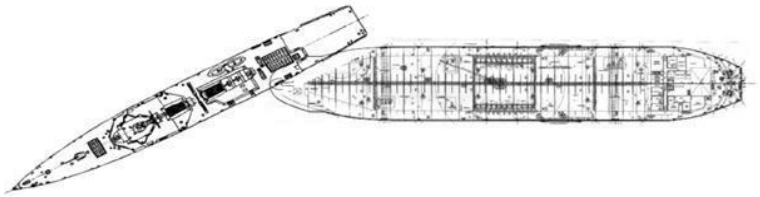


Figure 7 – Approximate Geometry and Point of Impact between USS JOHN S MCCAIN and ALNIC MC

Despite their close proximity, neither JOHN S MCCAIN nor ALNIC sounded the five short blasts of whistle required by the International Rules of the Nautical Road for warning one another of danger, and neither attempted to make contact through Bridge to Bridge communications.

3. IMPACT OF THE COLLISION

The bulbous bow of ALNIC MC impacted JOHN S MCCAIN on the port (left) aft side. The impact created a 28-foot diameter hole both below and above the waterline of the JOHN S MCCAIN. See Figures 7, 8, and 9.

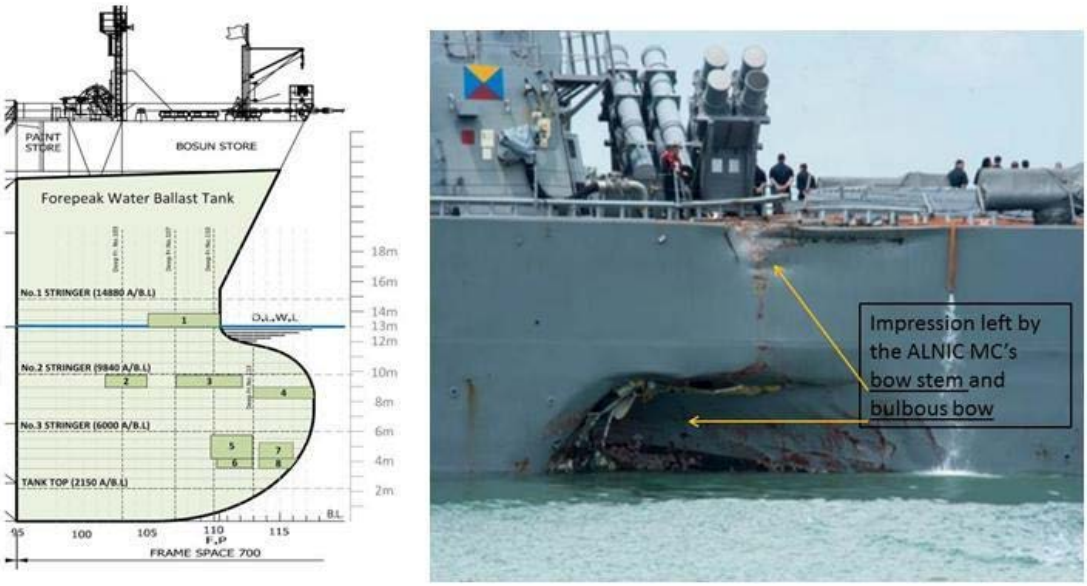


Figure 8 – Bulbous bow of Figure 9 – Point of impact on JOHN S MCCAIN ALINIC MC and damage to from ALINIC MC
hull from bow to stern

The point of impact was centered on Berthings 3 and 5 as noted in Figure 9. All significant injuries occurred to Sailors that were in Berthing 3 at the time of the impact. All ten of the fallen Sailors were in Berthing 5 at the time of impact.

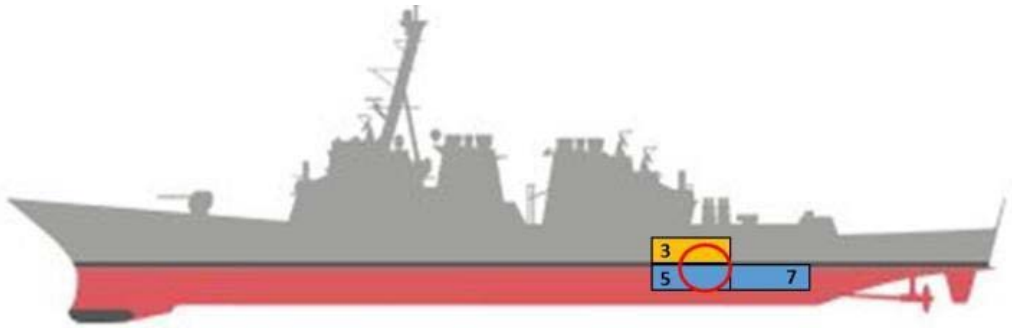


Figure 10 - Depiction of Approximate Location of Point of Impact

ALNIC MC and JOHN S MCCAIN initially remained attached to each other after the collision. Sailors describe this as lasting up to a couple of minutes. The prolonged contact kept the ship from taking a list (tilt to one side) immediately. Sailors on the bridge and on the external deck of the ship immediately after the collision could see ALNIC MC's bow (front of the ship) still lodged into the side of JOHN S MCCAIN. However, within 15 minutes JOHN S MCCAIN had developed a four degree list to port as the ship flooded.

The collision was felt throughout the ship. Watchstanders on the bridge were jolted from their stations momentarily and watchstanders in aft steering were thrown off their feet. Several suffered minor injuries. Some Sailors thought the ship had run aground, while others were concerned that they had been attacked. Sailors in parts of the ship away from the impact point compared it to an earthquake. Those nearest the impact point described it as like an explosion.

As required by Navy procedures, the Executive Officer ordered the collision alarm sounded to alert personnel to begin damage control efforts. The Commanding Officer remained on the bridge and the Executive Officer departed to the Combat Information Center and eventually to Berthing 3 to provide oversight in damage control efforts. The Command Master Chief, the senior assigned enlisted Sailor onboard, went to the area where damage control efforts, known as the Central Control Station, were managed and then moved about the ship, assisting damage control efforts. After the situation on the bridge stabilized, the Commanding Officer then proceeded to Central Control Station to check on the status of the damage control efforts.

The CO ordered the watch team to announce the collision on the Bridge-to-Bridge radio, which alerted other ships in the area to the collision and the damages. At 0530, JOHN S MCCAIN requested tugboats and pilots from Singapore Harbor to assist in getting the ship to Changi Naval Base.

JOHN S MCCAIN changed its lighting configuration at the mast to one red light over another red light, known as "red over red," the international lighting scheme that indicates a ship that is "not under command." Under the International Rules of the

Nautical Road, this warns other ships that, due to an exceptional circumstance, a vessel is unable to maneuver as required.

Most of the electronic systems on the bridge were inoperable until the two ships parted. Main communications systems on the bridge stopped working after the collision and the bridge began using handheld radios to communicate with aft steering. Sound powered phones, which do not require electrical power to transmit communications, and handheld radios were the main means of communication from the bridge. Aft Internal Communications, a space adjacent to Berthing 5 with communications control equipment, quickly flooded and was likely responsible for the loss of bridge communications.

All U.S. Navy ships are designed to withstand and recover from damage due to fire, flooding, and other damage sustained during combat or other emergencies. Each ship has a Damage Control Assistant, working under the Engineering Officer, in order to establish and maintain an effective damage control organization. The Damage Control Assistant oversees the prevention and control of damage including control of stability, list, and trim due to flooding (maintaining the proper level of the ship from side to side and front and back), coordinates firefighting efforts, and is also responsible for the operation, care and maintenance of the ship's repair facilities. The Damage Control Assistant ensures the ship's repair party personnel are properly trained in damage control procedures including firefighting, flooding and emergency repairs. The Damage Control Assistant is assisted by the Damage Control Chief (DCC), a chief petty officer specializing in Damage Control. The officer in charge of damage control efforts, the Damage Control Assistant, called away General Quarters to notify the crew to commence damage control efforts.

General Quarters is a process whereby the crew reports to pre-assigned stations and duties in the event of large casualties such as flooding. General Quarters is announced by an alarm that sounds throughout the ship to alert the crew of an emergency situation or potential combat operations. All crewmembers are trained to report to their General Quarters watch station and to set a higher condition of material readiness against fire, flooding, or other damage. This involves securing additional doors, hatches, scuttles, valves and equipment to isolate damage and prepare for combat. Navy crews train on Damage Control continuously, with drills being run in port and underway frequently to prepare the teams for damage to equipment and spaces. During any emergency condition (fire, flooding, combat operations), the Damage Control Assistant coordinates and supervises all damage control efforts from one of the three Damage Control Repair Lockers.

Damage Control Repair Lockers are specialized spaces stationed throughout the ship filled with repair equipment and manned during emergencies with teams of about 20 personnel trained to respond to casualties. There are three repair lockers on the JOHN S. MCCAIN: Repair Locker 2, Repair Locker 5, and Repair Locker 3. Repair Locker 2 covers the forward part of the ship, Repair Locker 5 covers the engineering spaces and Repair Locker 3 covers the aft part of the ship. Each locker is maintained with similar

equipment. Personnel assigned to repair lockers are trained and qualified to respond to and repair damage from a variety of sources with a specific focus on fire and flooding. Each repair locker can act independently but is also designed to support the others and can take over the responsibilities for any locker if damage prevents that locker's use. The repair lockers are normally unmanned unless the ship sets a condition of higher readiness like General Quarters when they would be manned within minutes.

Sailors began to locate, report and track flooding, fire, and structural damage to the ship immediately. Significant damage was reported throughout the ship in the moments after the collision, including flooding, internal fuel leakage, loss of ventilation and internal communications, and degradation of many of the ship's other systems.

JOHN S MCCAIN began the process of accounting for all crew members immediately after the collision. This process continued even as the crew made emergency repairs, battled flooding, and helped each other out of damaged spaces. The damage control efforts made confirming the location of personnel difficult. Varying reports of missing Sailors were made in the first minutes after the collision. However, by the submission of the third complete report, there was reasonable confidence that the crew had been accounted for was correct because all of the ten missing Sailors had been consistently reported missing and all lived in Berthing 5, a space that was inaccessible and flooded.

3.1 Impact to Berthing 5

Berthing 5 is located aft (near the back of the ship) on the port side. See Figure 10. It is approximately 25 feet by 15 feet and has 18 racks, stacked as bunk beds three-high. Each row of racks has a locker for Sailors' belongings. There is a lounge with seats, a small table, and a wall- mounted television. There is a head with one toilet, one shower stall, and one sink.

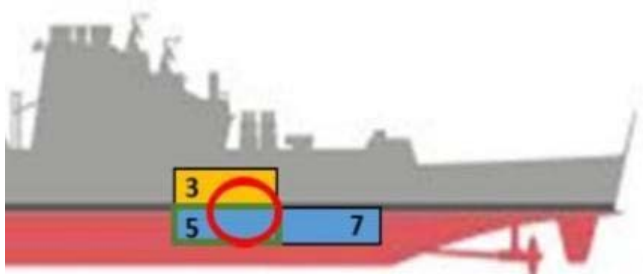


Figure 11 - Relative Positions of Berthings 3, 5 (in green), and 7, and point of impact

There are two means to exit Berthing 5: the primary egress (ladderwell) through a hatch with a scuttle (Figure 11) and an escape scuttle into Berthing 3 on the deck above (Figure 12).

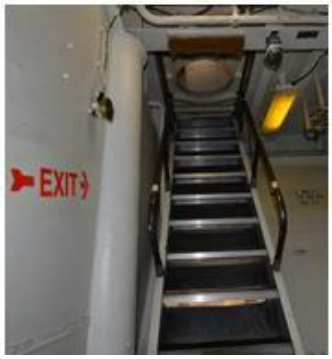


Figure 12 – Primary egress from Berthing 5 Figure 13 – Escape Scuttle from Berthing 5

During Modified ZEBRA, the hatch is closed, but the scuttle is open for ease of access. The escape scuttle is normally closed at all times, as it was at the time of the impact. The collision knocked debris in Berthing 3 on top of the escape scuttle connecting Berthing 3 to Berthing 5 below it. This would have made any attempts to open and exit through the escape scuttle very difficult.

Most of the Berthing 5, a space that is normally 15 feet wide, was compressed by the impact to only 5 feet wide. There were 17 Sailors assigned to Berthing 5. At the time of the collision, all were aboard the ship and five were on watch or outside the space. Based on the size of the hole, and the fact that Berthing 5 is below the waterline, the space likely fully flooded in less than a minute after the collision.

Two Sailors who were in Berthing 5 at the time of the collision escaped from the space. The first Sailor was on the second step of the ladder-well leading to the deck above when the collision occurred. The impact of the collision knocked him to the ground, leaving his back and legs bruised. Fuel quickly pooled around him and he scrambled up and back onto the ladder. The Sailor climbed out of Berthing 5 through the open scuttle, covered in fuel and water from the near instantaneous flooding of the space. He did not see anyone ahead of or behind him as he escaped. He reported seeing two other Sailors in the lounge area, one preparing for watch duties and another standing near his rack. Both of these Sailors were lost, along with the eight shipmates who were in their racks to rest at the time of the collision.

The second Sailor who escaped from Berthing 5 heard the crashing and pushing of metal before the sound of water rushing in. Within seconds, water was at chest level. The passageway leading to the ladder-well was blocked by debris, wires and other wreckage hanging from the overhead. From the light of the battle lanterns (the emergency lighting that turns on when there is a loss of normal lights due to power outage) he could see that he would have to climb over the debris to get to the ladder-well.

As he started his climb across the debris to the open scuttle, the water was already within a foot of the overhead, so he took a breath, dove into the water, and swam towards the ladder-well. Underwater, he bumped into debris and had to feel his way along. He was able to stop twice for air as he swam, the water higher each time, and eventually used the pipes to guide him towards the light coming from the scuttle. The Sailor found that the blindfolded egress training, a standard that requires training to prepare Sailors for an emergency and was conducted when he reported to the command, was essential to his ability to escape.

One Sailor was alerted by the first Sailor who escaped Berthing 5 that others were still inside the space, and he went to assist them. When he first reached the closed hatch and open scuttle, the water in Berthing 5 was at the top of the third rung. He tried to enter the space, but was forced back up the ladder by the pressure of the escaping air and rising water, which within seconds had risen to within a foot of the hatch. He saw a Sailor swimming toward the exit and pulled him out of the water through the scuttle between the two decks. This was the second and last Sailor to escape from Berthing 5. His body was scraped, bruised, and covered with chemical burns from being submerged in the mixture of water and fuel.

An additional Sailor who came to assist observed the rescue and, looking down into the berthing, saw “a green swirl of rising seawater and foaming fuel” approaching the top of the scuttle. As the final Sailor to leave Berthing 5 was pulled to safety, the Sailors at the top of the scuttle checked to see if there was anyone behind him. They did not see anybody. By then, so much water was already coming up through the scuttle that it was difficult to close and secure. The fuel mixed in with the water made one of Sailor’s hands so slippery that he cut himself while using the wrench designed to secure the scuttle, but the two were able to secure it to stop the rapid flooding of the ship.

3.2 Impact on Berthing 3

Berthing 3 is immediately above Berthing 5, but spans the width of the ship. There are two points of egress from each side of Berthing 3; on the port side there is a ladder-well leading down into the center of the berthing and an escape scuttle that is located in the forward section of the space leading up to the next deck. There were 71 Sailors assigned to Berthing 3.

At 0530, the DCA began receiving reports of a ruptured fire main and water and fuel flooding into Berthing 3. The port side of Berthing 3 suffered substantial damage, including a large hole in the bulkhead. See Figure 13. Racks and lockers detached from the walls and were thrown about, leaving jagged metal throughout the space. Cables and debris hung from the ceiling.

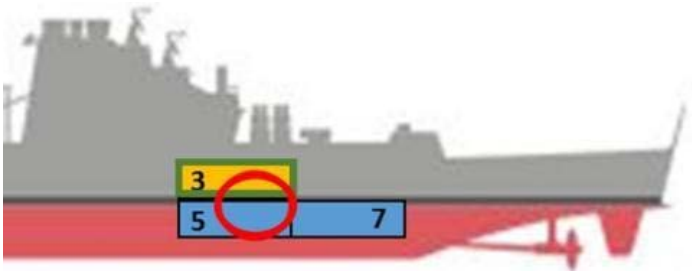


Figure 14 - Relative Positions of Berthings 3, 5, and 7 and point of impact

A Sailor from Berthing 3, who was later medically evacuated from the ship, sustained his injuries as the wall next to him blew apart in the collision and threw him to the ground. Water and fuel quickly pooled around him in the short time he was on the ground, and he began crawling over debris to escape. Another Sailor went to him and helped pull him to the lounge area and toward the ladder. On the way, the Sailor who was being assisted fell on the slippery floor and hit his head. Two other Sailors, also injured, helped him reach the flight deck.

Limited lighting guided the remaining Sailors as they left the berthing space. Sailors had to climb over lockers and other debris to escape, using the high vantage point to also minimize the risk of electrocution from traveling through the rising water. Some escaped in only their underwear, and many were bruised and bloodied from injuries sustained in the collision and covered in fuel. At least one Sailor attempted to move the metal rack pinning a trapped shipmate, and realized that he could not move it alone. The Sailors who escaped Berthing 3 provided some of the first reports to CCS that the space was severely damaged, that it was rapidly taking on water, and that Sailors were trapped inside.

Hearing reports that Sailors were trapped in Berthing 3, the Executive Offer and a group of Sailors, including some who evacuated Berthing 7, went to check on their shipmates. Several Sailors were pinned in their racks as a result of the collision, but, as the two ships pulled apart, the twisted metal shifted and most of the Sailors in Berthing 3 were able to escape as the debris moved. One of these Sailors was pinned in his rack underneath two racks that had collapsed and a number of lockers that became dislodged during the collision. He was able to escape after ALNIC MC detached. See Figures 14 and 15.

Figure 15 – Berthing 3 facing port Figure 16 – Berthing 3 facing port after collision

However, two Sailors remained pinned in their racks even after the ships separated. Four members of the crew entered Berthing 3 through the jagged metal and rising water to rescue them. The first of these rescuers heard Sailors shouting for help from inside Berthing 3 and tried to enter on the port side; however, the door was blocked by debris, so he ran to the entrance on the starboard (right) side of the berthing.

One of the Sailors trapped in Berthing 3 had been asleep at the time of the collision and was awoken by it. When he opened his eyes, he understood that he was pinned in his rack, with one of his shoulders stuck between his rack and the rack above. He felt both air and water moving around him. He could hear shouting and began shouting himself, which alerted his others that he was trapped. Only his hand and foot were visible by those outside of the rack. The one battle lantern in the area provided the only light for rescuers to find the trapped Sailor. Water was already at knee level when rescuers reached him. The debris was too heavy for the rescuers to move, and a Portable Electric All-Purpose Rescue System, a “jaw of life” cutting device, was required to cut through the metal, separate the panels of the rack, and pull the panels out of the way. After approximately 30 minutes, these efforts allowed the trapped Sailor to pull his arm free. Moments later, the rescuers pulled him from between the racks by his foot. Stretcher bearers came to Berthing 3 and carried this Sailor to the Mess Decks to receive medical treatment.

The second Sailor was in a bottom rack in Berthing 3. His rack was lifted off the floor as a result of the collision, which likely prevented him from drowning in the rising water, and he was trapped at an angle between racks that had been pressed together. Light was visible through a hole in his rack and he could hear the water and smell the fuel beginning to fill Berthing 3.

He attempted to push his way out of the rack, but every time he moved the space between the racks grew smaller and he was unable to escape. His foot was outside the rack and he could feel water. It was hot in the space and difficult to breathe, but he managed to shout for help and banged against the metal rack to get the attention of other Sailors in the berthing space. The Sailors who entered Berthing 3 to rescue others heard this and began assisting him, but he was pinned by more debris than the first Sailor freed.

It took approximately an hour from the time of the collision to free the second Sailor from his rack. Rescuers used an axe to cut through the debris, a crow bar to pull the lockers apart piece by piece, and rigged a pulley to move a heavy locker in order to reach the Sailor. Throughout the long process, his rescuers assured him by touching his foot, which was still visible. Once freed, the Sailor was the last person to escape Berthing 3. Everything aft of his rack was a mass of twisted metal. He had scrapes and bruises all over his body, suffered a broken arm, and had hit his head. He was unsure whether he remained conscious throughout the rescue.

At least one scuttle to Berthing 3 was shut during damage control efforts. The space was electrically isolated and, at 0608, the fire main valves were closed, reducing the amount of flooding. Dewatering efforts began and succeeded in removing the water from Berthing 3 prior to JOHN S MCCAIN's arrival at Changi Naval Base.

3.3 Impact on Berthings 4, 6, and 7

Berthings 5 and 7 are next to each other on the port side of the ship, mirrored by Berthings 4 and 6, respectively, on the starboard side of the ship. Berthings 4 and 5 are connected across the ship through "cross flooding ducts," designed to distribute water from port to starboard side (or vice versa) to keep the ship level if it takes on water. Berthings 6 and 7 are similarly connected. A six foot long crack in the wall between Berthings 5 and 7, created by the collision, allowed water to move between the spaces.

All Sailors in Berthing 7 were able to evacuate, but water was at approximately knee level as they exited the space. At 0530 there was report of a ruptured pipe in Berthing 7, which added to the flooding caused by the cracked wall separating Berthings 5 and 7. By 0605, Berthing 7 was reported as lost, meaning that it was fully flooded and secured to prevent the flooding from spreading to the rest of the ship.

All Sailors in Berthing 4 were able to evacuate. At 0544, Sailors reported 4 inches of water on the deck in Berthing 4. Sailors in Berthing 4 were thrown about their racks by the force of the collision. By 0627, the berthing space was lost. See Figures 16 and 17.

Figure 17—Scuttle and hatch into Figure 18—Berthing 4 racks after Berthing 4 showing the space dewatering completely flooded

All Sailors in Berthing 6 were able to evacuate. At 0546 flooding was reported in Berthing 6, which is across from Berthing 7 on the starboard side of the ship. Despite the crew's dewatering efforts, the space was declared lost at 0627.

At approximately 0630, as a result of crew's resiliency and successful damage control and engineering repair efforts, JOHN S MCCAIN was able to proceed under its own power toward Changi Naval Base, Singapore, at an average speed of 3 knots. JOHN S MCCAIN's navigation equipment was degraded as a result of the collision. While most electronic navigational aids on the bridge were operational, multiple warnings and alerts were illuminated, reducing the navigation team's confidence that the information was reliable. Because of the degraded information, the team relied on "seaman's eye" to stay on track while returning to port. Lack of ventilation across the ship raised concerns based on the amount of fuel that had spilled and the risks posed by rising temperatures inside the ship. The temperatures also drove many Sailors to the flight deck in order to escape the heat.

4. MEDICAL EFFORTS AND INJURIES

JOHN S MCCAIN medical teams established a triage center in Messing. This space, where the crew eats their meals, provided the largest open space on the ship and medical procedures can be performed on the cafeteria-style tables. The medical team treated lacerations and chemical burns from fuel exposure, splinted broken bones, and provided broad spectrum antibiotics to Sailors with open wounds. Triage care moved back to the Medical office at approximately 0630, as the initial rush of patients had been treated so the medical team would have full access to their equipment and supplies.

At approximately 0915, as the ship was transiting to Changi Naval Base, four seriously injured Sailors were medically evacuated to Singapore General Hospital by helicopter. Once pier-side at Changi Naval Base, another Sailor was transported to the hospital because of shock symptoms and an injury to his shoulder. This Sailor was one of

the Sailors who had been trapped in Berthing 3. Three of the five medically evacuated Sailors were transported from Singapore to Yokosuka, Japan on 27 August 2017. The remaining two were transported back to Yokosuka, Japan on 28 August 2017.

As JOHN S MCCAIN approached Changi Naval Base, AMERICA approached alongside and two members of AMERICA's medical team came aboard to provide additional support, including intravenous fluids to treat heat stroke. Once the ships were pier side, AMERICA hosted the JOHN S MCCAIN medical team, together treating Sailors with cuts and chemical burns from fuel exposure. Until alternative arrangements could be made, AMERICA also provided meals for all JOHN S MCCAIN Sailors and berthing for over 150 Sailors whose berthings were flooded. The Sailors and Marines aboard AMERICA also provided initial support for the JOHN S MCCAIN crew, including daily supplies, watchstanders, counseling, and communications network support.

In total, 48 Sailors suffered injuries that required medical treatment. Five Sailors who were treated at Singapore General Hospital suffered severe injuries and were unable to return to their duties for more than 24 hours. Of the 48 injured Sailors, 43 continued to assist with damage control and recovery efforts immediately following the collision.

5. SEARCH AND RESCUE EFFORTS - 21 TO 24 AUGUST 2017

Though the ship did not have a complete muster confirming ten Sailors were missing until 0715, JOHN S MCCAIN reported that Sailors were believed missing within moments of the collision. Coordination began immediately for search and rescue (SAR) efforts in the water space surrounding the collision site.

At approximately 0715 on 21 August 2017, SAR Operations commenced with Commander, Amphibious Squadron 3 (CPR 3) as SAR On-Scene Commander. At approximately 0700, AMERICA was enroute and preparing to launch MV-22B Ospreys and MH- 60S Sea Hawks to support SAR efforts once in range. Republic of Singapore Navy (RSN) and Republic of Singapore Coast Guard (RSNCG) SAR units were on station by 0800. Eventually there would be six Singaporean and six Malaysian vessels searching near the collision site.

At approximately 0900, the Republic of Singapore (RSN) deployed three ships with damage control equipment to assist and transfer equipment to JOHN S MCCAIN on a rigid-hulled inflatable boat (RHIB).

At approximately 1000 and 1030, two helicopters from AMERICA landed on the deck of JOHN S MCCAIN with damage control equipment and in support of the SAR efforts. By approximately 1400, U.S. Navy aircraft were conducting SAR efforts within 25nm of the collision point. A RSN helicopter, two RSN patrol boats, and a RSNCG vessel were on scene to assist.

The Malaysian Navy and RSN both searched 10nm on either side of the path that JOHN S MCCAIN had traveled, attempting to locate any Sailors that may have fallen through the hole in the ship's hull made by the collision. Throughout the evening of 21 August 2017, and continuously until 2000 on 24 August 2017, aircraft and surface vessels from the U.S. Navy, RSN, RSNCG, Singapore Air Force, Singapore Maritime Port Authority, Royal Malaysian Navy, Malaysian Maritime Enforcement Agency, Indonesian Navy and Royal Australian Air Force conducted multinational SAR operations. These efforts were coordinated from AMERICA, lasting for more than 80 hours and spanning more than 2,100-square miles.

On 22 August 2017, a body was found in the water by Malaysian units assisting the SAR efforts. The body was determined not to be one of the Sailors missing from JOHN S MCCAIN. SEVENTH Fleet suspended all SAR efforts outside the hull of JOHN S MCCAIN at sunset on 24 August 2017. Recovery efforts inside the hull of the ship continued.

6. DIVING AND RECOVERY OPERATIONS

A team of Navy Divers arrived on JOHN S MCCAIN as the ship entered the harbor in Singapore at approximately 1200 on 21 August 2017. They began inspecting the ship to determine how best to proceed with a dive inside the ship. The leader of the dive team inspected Berthing 3 and saw waves breaking into the ship. The divers discovered the hole in the port side of JOHN S MCCAIN that was approximately 28 feet wide. See Figure 18.

Figure 19 – Port side of JOHN S MCCAIN post-collision

By approximately 1435, JOHN S MCCAIN was moored and divers were in the water looking for places to enter the hull of the ship. The hole in the port side penetrated

not only the hull, but an internal fuel tank as well. The fuel in the water created a number of hazards to divers and required them to proceed cautiously.

On a second dive at approximately 1500, divers were able to enter the hull of the ship to do initial safety assessments. Many of the conditions they found led to a cautious approach to assure the safety of the divers. The large amount of debris and structural damage required the divers to move slowly about the ship, even cutting holes through racks to access parts of the space. Visibility in Berthing 5 was very poor given the debris and lack of light. The divers had to move about the space almost exclusively by feel. The dive team conducted nearly continuous dive operations over a period of seven days until all ten of the Sailors in Berthing 5 were recovered.

7. FINDINGS

Collisions at sea are rare and the relative performance and fault of the vessels involved is an open admiralty law issue. The Navy is not concerned about the mistakes made by ALNIC. Instead, the Navy is focused on the performance of its ships and what we could have done differently to avoid these mishaps.

In the Navy, the responsibility of the Commanding Officer for his or her ship is absolute. Many of the decisions made that led to this incident were the result of poor judgment and decision making of the Commanding Officer. That said, no single person bears full responsibility for this incident. The crew was unprepared for the situation in which they found themselves through a lack of preparation, ineffective command and control and deficiencies in training and preparations for navigation.

7.1 Training

From the time when the CO ordered the Helm and Lee Helm split, to moments just before the collision, four different Sailors were involved in manipulating the controls at the SCC.

Because steering control was in backup manual at the helm station, the offer of control existed at all the other control stations (Lee Helm, Helm forward station, Bridge Command and Control station and Aft Steering Unit). System design is such that any of these stations could have taken control of steering via drop down menu selection and the Lee Helm's acceptance of the request. If this had occurred, steering control would have been transferred.

When taking control of steering, the Aft Steering Helmsman failed to first verify the rudder position on the After Steering Control Console prior to taking control. This error led to an exacerbated turn to port just prior to the collision, as the indicated rudder position was 33 degrees left, vice amidships. As a result, the rudder had a left 33 degrees order at the console at this time, exacerbating the turn to port.

Several Sailors on watch during the collision with control over steering were temporarily assigned from USS ANTIETAM (CG 54) with significant differences between the steering control systems of both ships and inadequate training to compensate for these differences.

Multiple bridge watchstanders lacked a basic level of knowledge on the steering control system, in particular the transfer of steering and thrust control between stations. Contributing, personnel assigned to ensure these watchstanders were trained had an insufficient level of knowledge to effectively maintain appropriate rigor in the qualification program. The senior most officer responsible for these training standards lacked a general understanding of the procedure for transferring steering control between consoles.

7.2 Seamanship and Navigation

Much of the track leading up to the Singapore Traffic Separation Scheme was significantly congested and dictated a higher state of readiness. Had this occurred, maximum plant reliability could have been set with a Master Helmsman and a qualified Engineering Lee Helm on watch.

If the CO had set Sea and Anchor Detail adequately in advance of entering the Singapore Strait Traffic Separation Scheme, then it is unlikely that a collision would have occurred. The plan for setting the Sea and Anchor Detail was a failure in risk management, as it required watch turnover of all key watch stations within a significantly congested TSS and only 30 minutes prior to the Pilot pickup.

If JOHN S MCCAIN had sounded at five short blasts or made Bridge-to-Bridge VHF hails or notifications in a timely manner, then it is possible that a collision might not have occurred.

If ALNIC had sounded at least five short blasts or made Bridge-to-Bridge VHF hails or notifications, then it is possible that a collision might not have occurred.

7.3 Leadership and Culture

The Commanding Officer decided not to station the Sea and Anchor detail when appropriate, despite recommendations from the Navigator, Operations Officer and Executive Officer.

Principal watchstanders including the Officer of the Deck, in charge of the safety of the ship, and the Conning Officer on watch at the time of the collision did not attend the Navigation Brief the afternoon prior. This brief is designed to provide maximum awareness of the risks involved in the evolution.

Leadership failed to provide the appropriate amount of supervision in constructing watch assignments for the evolution by failing to assign sufficient experienced officers to duties.

The Commanding Officer ordered an unplanned shift of thrust control from the Helm Station to the Lee Helm station, an abnormal operating condition, without clear notification.

No bridge watchstander in any supervisory position ordered steering control shifted from the Helm to the Lee Helm station as would have been appropriate to accomplish the Commanding Officer's order. As a result, no supervisors were aware that the transfer had occurred.

Senior officers failed to provide input and back up to the Commanding Officer when he ordered ship control transferred between two different stations in proximity to heavy maritime traffic.

Senior officers and bridge watchstanders did not question the Helm's report of a loss of steering nor pursue the issue for resolution.

LIST OF REFERENCES

[1] D. M. Turek, “Explainable Artificial Intelligence (XAI),” Defense Advanced Research Projects Agency, Accessed 25 July 2020. [Online]. Available: https://www.darpa.mil/program/explainable-artificial-intelligence.

[2] N. G. Leveson, *Safeware: System Safety and Computers*, Boston, MA, USA: Addison-Wesley Publishing Company, 1995.

[3] N. G. Leveson, *Engineering a Safer World*, Cambridge, MA, USA: MIT Press, 2017.

[4] Chief of Naval Operations, *Operational Risk Management*, Washington, DC, USA: U.S. Navy, 2010.

[5] Office of Safety and Mission Assurance, “System Safety,” National Aeronautics and Space Administration, 28 July 2020. [Online]. Available: https://sma.nasa.gov/sma-disciplines/system-safety.

[6] National Transportation Safety Board, *Collision between U.S. Navy Destroyer USS JOHN S MCCAIN and Tanker Alnic MC, Singapore Strait*, Washington, DC, USA: National Transportation Safety Board, 2017.

[7] Chief of Naval Operations, *Report on the Collision between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC*, Washington, DC, USA: U.S. Navy, 2017.

[8] United States Fleet Forces Command, *Comprehensive Review of Recent Surface Forces Incidents*, Norfolk, VA, USA: U.S. Navy, 2017.

[9] J. Stavridis and R. Girrier, *Watch Officers Guide* (Fifteenth Edition), Annapolis, MD, USA: Naval Institue Press, 2007.

[10] International Maritime Organization, *Convention on the International Regulations for Preventing Collisions at Sea*, London, England, UK: International Maritime Organization, 1972.

[11] T. C. Miller, M. Rose, R. Faturechi and A. Chang, “Collision Course,” 20 December 2019. ProPublica. [Online]. Available: https://features.propublica.org/navy-uss-mccain-crash/navy-installed-touch-screen-steering-ten-sailors-paid-with-their-lives/

[12] M. Eckstein, “Navy Reverting DDGs Back to Physical Throttles, After Fleet Rejects Touchscreen Controls,” USNI. 09 August 2019. [Online]. Available: https://news.usni.org/2019/08/09/navy-reverting-ddgs-back-to-physical-throttles-after-fleet-rejects-touchscreen-controls

[13] Merriam-Webster, “Context,” Accessed 02 September 2020. [Online]. Available: https://www.merriam-webster.com/dictionary/context

[14] Merriam-Webster, “Awareness,” Accessed 02 Month 2020. [Online]. Available: https://www.merriam-webster.com/dictionary/awareness

[15] A. K. Dey and G. D. Abowd, *A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications*, *Atlanta*, GA, USA: Georgia Institute of Technology, 2001.

[16] J. Bisgaard, M. Heise and C. Steffensen, *How IsContext and Contex-awareness Defined and Applied? A Survey of Context-awareness,* Aalborg East, Denmark: Aalborg University, 2005.

[17] A. Schmidt, “Interaction Design Foundation,” Interaction-Design. Accessed 10 January 2020. [Online]. Available: https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/context-aware-computing-context-awareness-context-aware-user-interfaces-and-implicit-interaction

[18] J. Wagner, “Evolution of a Modern Naval Steering System,” *Naval Engineers Journal*, no. May, pp. 55–64, 1987.

[19] A. Marshall, “No More Screen Time! The Navy Reverts to Physical Throttles,” Wired, 14 August 2018. [Online]. Available: https://www.wired.com/story/no-more-screen-time-navy-reverts-physical-throttles/.

[20] Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy,* Washington, DC, USA: Department of Defense, 2019.

[21] M. Wieringa, “What to Acount For When Accounting For Algorithms,” *Fairness, Accountability, and Transparency,* pp. 12–17, 2020.

[22] J. Konrad, “Bridge Resource Management – A New Focus On Watchkeeping,” gCaptain, 11 November 2007. [Online]. Available: https://gcaptain.com/cosco-busan-bridge-resource-management/.

[23] U.S. Department of Defense, *DOD Adopts Ethical Principles for Artificial Intelligence*, Washington, DC, USA: U.S. Department of Defense, 2020.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California